ORACLE

Oracle Audit Vault and Database Firewall

Overview

Alexandre Fagundes
Marcel Lamarca

LAD Partner Enablement

Topics

1 Overview and use cases

2 Database auditing and audit data collection

3 Network-based SQL traffic monitoring

4 Alerts and reports

5 Enterprise deployment

6 Supported targets and configurations

7 Summary

Oracle Audit Vault and Database Firewall

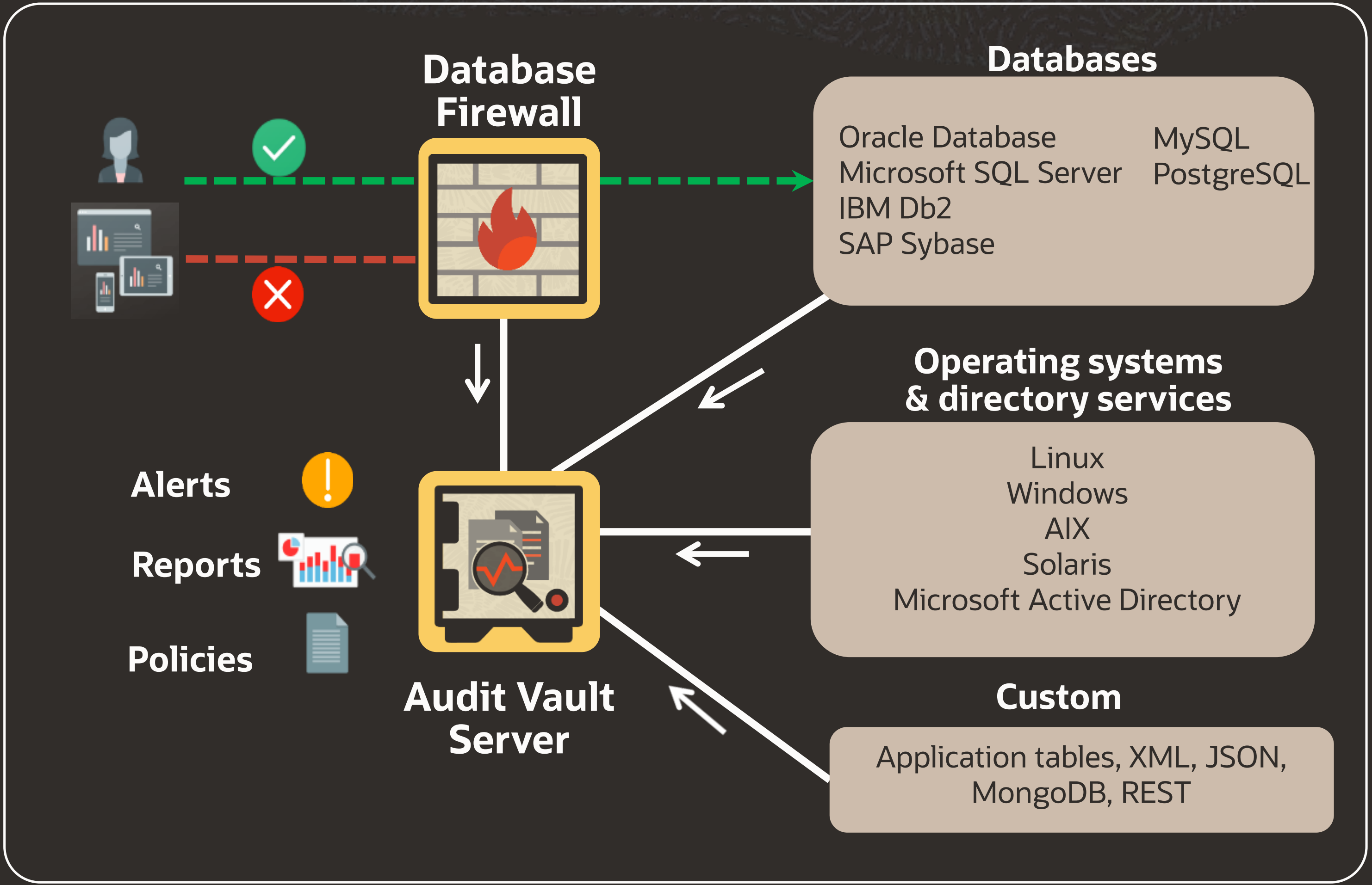
— Oracle Audit Vault and Database Firewall is a comprehensive and scalable software solution for database auditing and network-based activity monitoring.

Protect Your Data & Applications

- Implement corporate security policies relating to activity monitoring and auditing
- Monitor and audit privileged user access to sensitive data
- Enforce trusted path access to corporate applications
- Blocking and monitoring of SQL statements

Accelerate Regulatory Compliance

- Address compliance requirements e.g.: PCI, HIPAA, GDPR, etc.
- Pre-defined compliance reports
- Support forensic analysis



Key features

Database auditing and audit collection

- Audit collection including data access and modification
- Before/after values, entitlement changes , stored procedure changes
- Application auditing with custom collectors
- Seeded audit policies for Oracle

SQL traffic monitoring using database firewall

- Multi-stage firewall using SQL grammar analysis
- Policies based on session parameters, database objects, SQL clusters
- SQL Injection detection and prevention

Reporting and alerting

- Powerful, customizable reports with filtering for forensic analysis
- Out-of-the-box reports for security and compliance
- Rich alert builder to detect unexpected activity
- Open schema enabling integration with third party tools

Enterprise deployment

- Auto updatable agents for easier management
- Automated archival of audit data for compliance
- LDAP/Active Directory authentication
- Single console for managing audit and network monitoring
- SIEM/Syslog integration
- High availability for continuous audit collection
- Delivered as full-stack software appliance

Supported target types and configurations

- Heterogeneous target types - Oracle and non-Oracle databases, operating system logs, directory service, file systems
- Extensible with custom collector framework (table, XML, JSON, REST)
- Hybrid cloud deployments

Database auditing and audit data collection

Database auditing and monitoring use cases

Monitoring all privileged user activity

Operations on sensitive data

Before / after data value changes

Login failures

Entitlement changes

Stored procedure changes

Compliance related reporting for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, UK DPA

Database audit collection with AVDF

Configure targets and trails

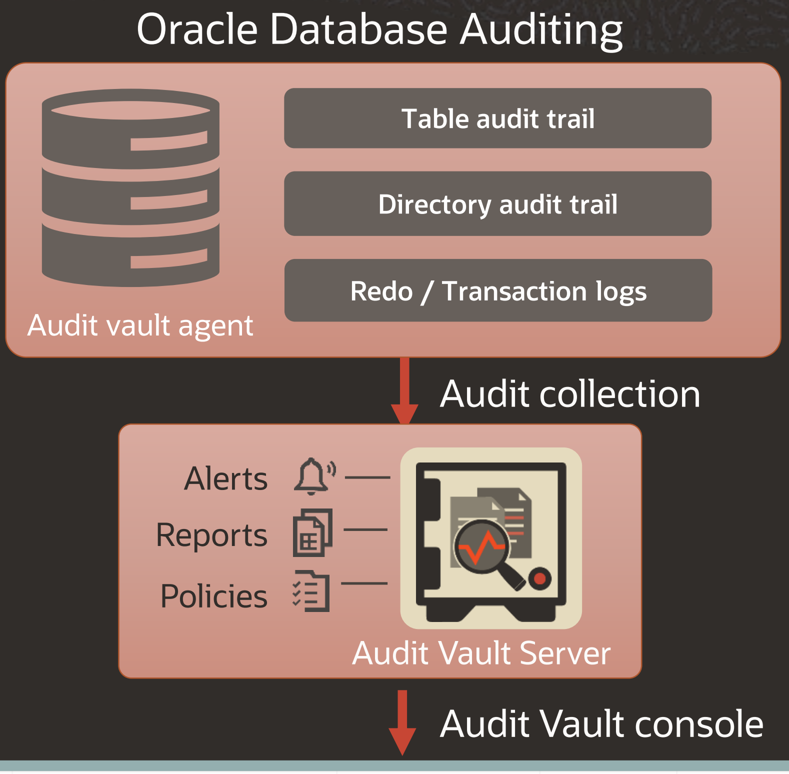
- Targets
- Audit vault agents
- Audit data collection (trails)
- Data retention policy

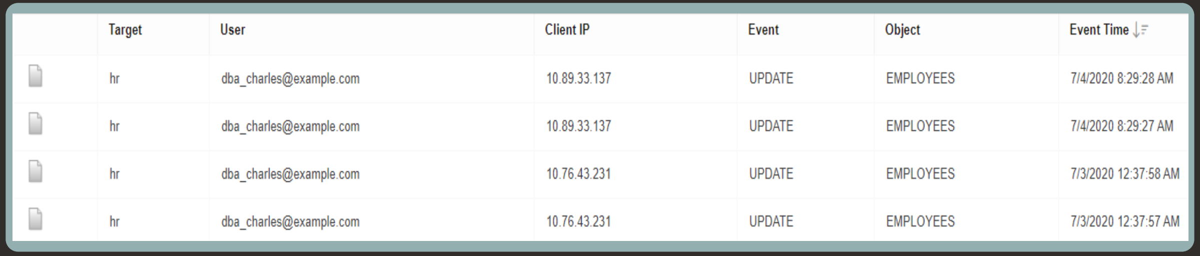
Configure audit policies

- Who
- What
- When
- Where

Create reports and alerts

- Define alert baselines
- Create and schedule reports





	Target	User	Client IP	Event	Object	Event Time
	hr	dba_charles@example.com	10.89.33.137	UPDATE	EMPLOYEES	7/4/2020 8:29:28 AM
	hr	dba_charles@example.com	10.89.33.137	UPDATE	EMPLOYEES	7/4/2020 8:29:27 AM
	hr	dba_charles@example.com	10.76.43.231	UPDATE	EMPLOYEES	7/3/2020 12:37:58 AM
	hr	dba_charles@example.com	10.76.43.231	UPDATE	EMPLOYEES	7/3/2020 12:37:57 AM

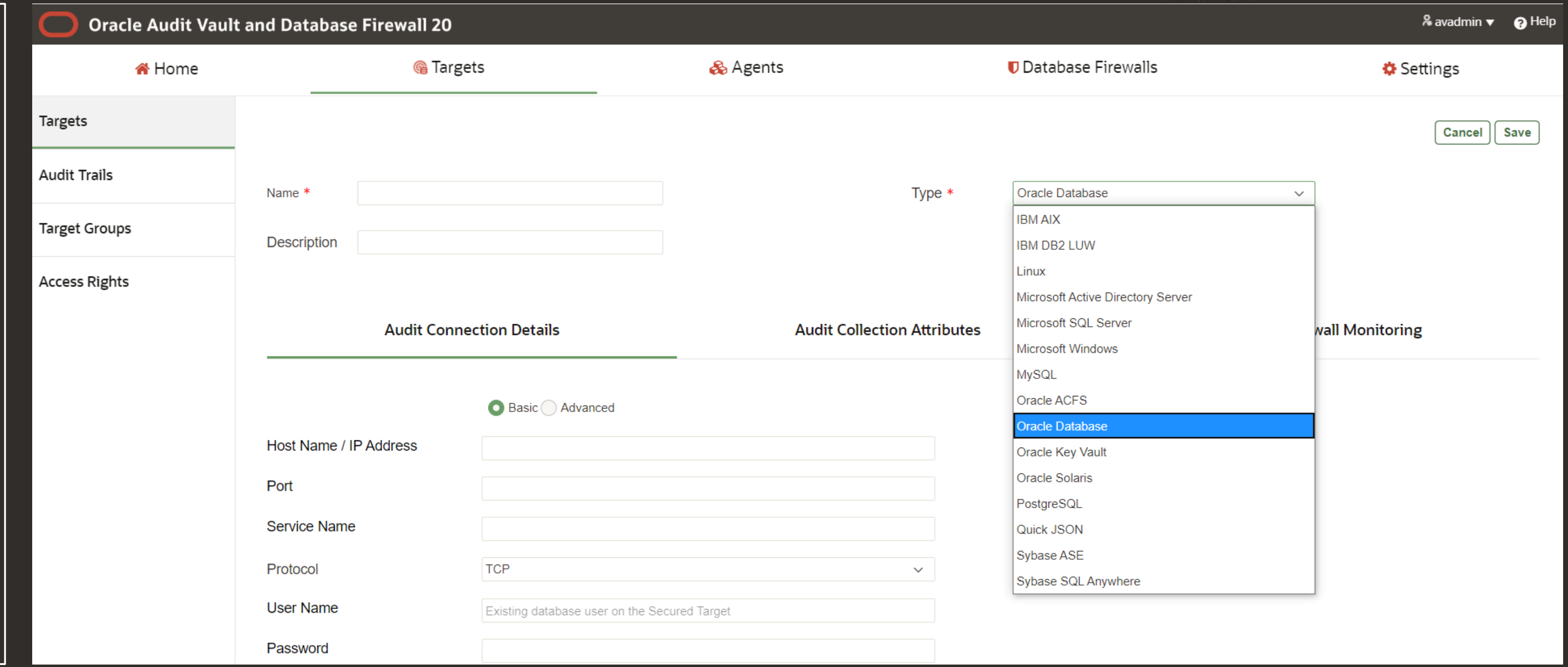
Registering Targets and Audit Trails

Registering Targets

Select from pre-defined target type

Add Trails (sources of audit data)

Table, Directory, Transaction Log, etc.



Name *

Description

Type * Oracle Database

- IBM AIX
- IBM DB2 LUW
- Linux
- Microsoft Active Directory Server
- Microsoft SQL Server
- Microsoft Windows
- MySQL
- Oracle ACFS
- Oracle Database
- Oracle Key Vault
- Oracle Solaris
- PostgreSQL
- Quick JSON
- Sybase ASE
- Sybase SQL Anywhere

● Basic ○ Advanced

Host Name / IP Address

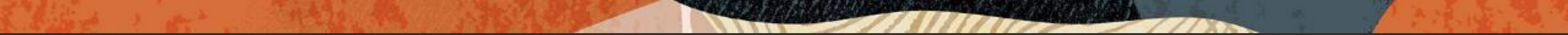
Port

Service Name

Protocol TCP

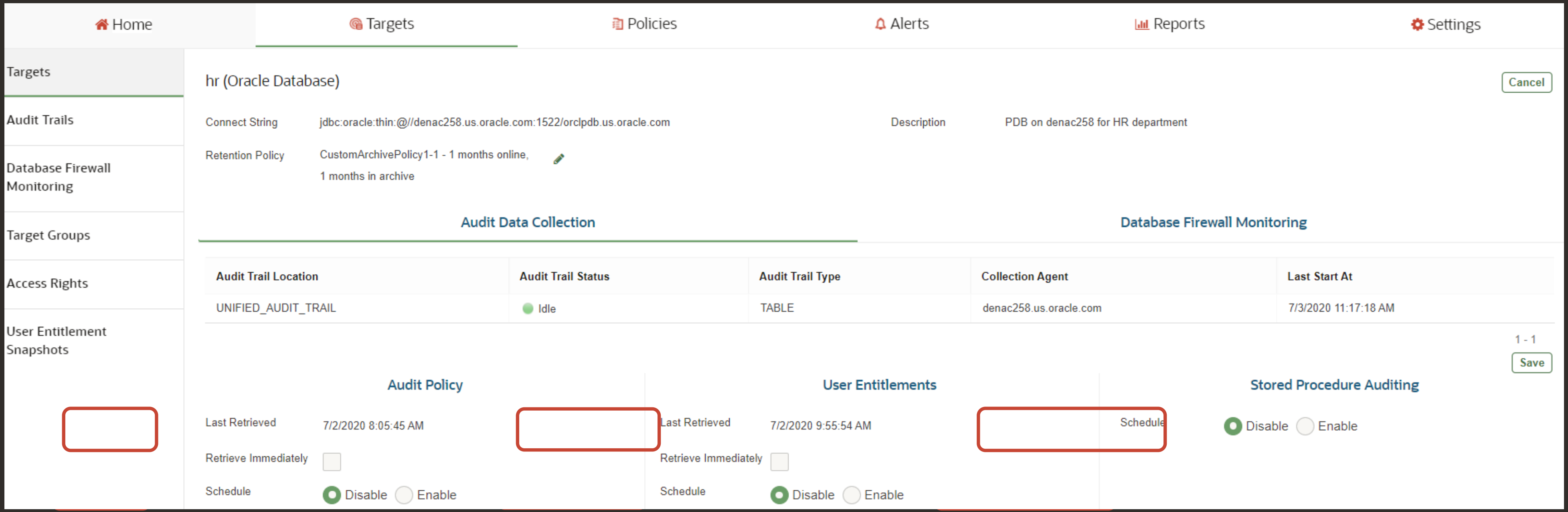
User Name Existing database user on the Secured Target

Password



Audit and entitlement data collection

- Audit policy
- User entitlements
- Stored procedure changes



hr (Oracle Database)

Connect String jdbc:oracle:thin:@//denac258.us.oracle.com:1522/orclpdb.us.oracle.com

Description PDB on denac258 for HR department

Retention Policy CustomArchivePolicy1-1 - 1 months online, 1 months in archive

Audit Trail Location	Audit Trail Status	Audit Trail Type	Collection Agent	Last Start At
UNIFIED_AUDIT_TRAIL	● Idle	TABLE	denac258.us.oracle.com	7/3/2020 11:17:18 AM

Audit Policy

Last Retrieved 7/2/2020 8:05:45 AM

Retrieve Immediately □

Schedule ● Disable ○ Enable

User Entitlements

Last Retrieved 7/2/2020 9:55:54 AM

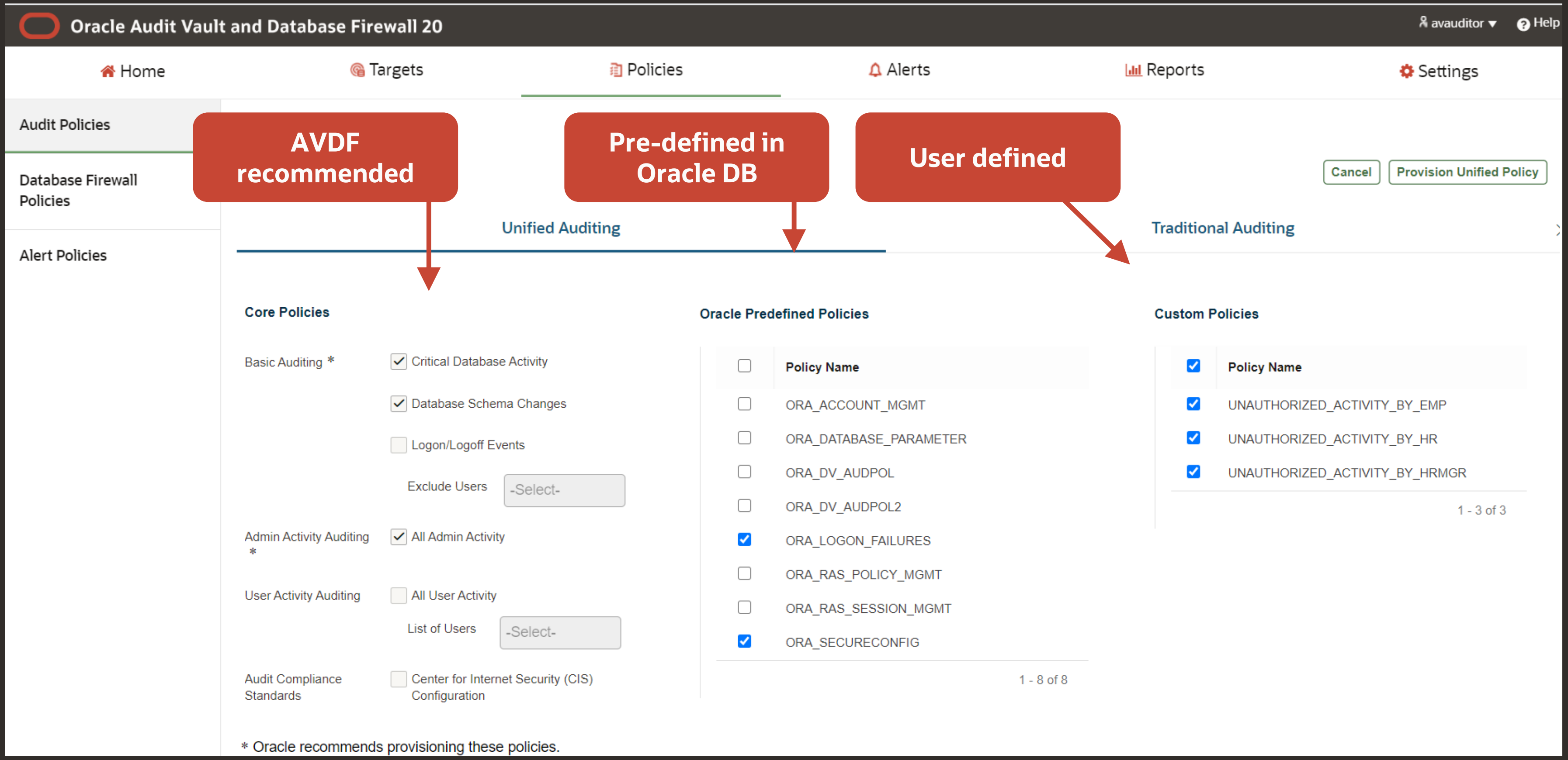
Retrieve Immediately □

Schedule ● Disable ○ Enable

Stored Procedure Auditing

Schedule ● Disable ○ Enable

New: default seeding of audit policies for Oracle



AVDF recommended

Pre-defined in Oracle DB

User defined

Core Policies

Basic Auditing *
- ☑ Critical Database Activity
- ☑ Database Schema Changes
- □ Logon/Logoff Events
- Exclude Users: -Select-

Admin Activity Auditing *
- ☑ All Admin Activity

User Activity Auditing
- □ All User Activity
- List of Users: -Select-

Audit Compliance Standards
- □ Center for Internet Security (CIS) Configuration

Oracle Predefined Policies

□	Policy Name
□	ORA_ACCOUNT_MGMT
□	ORA_DATABASE_PARAMETER
□	ORA_DV_AUDPOL
□	ORA_DV_AUDPOL2
☑	ORA_LOGON_FAILURES
□	ORA_RAS_POLICY_MGMT
□	ORA_RAS_SESSION_MGMT
☑	ORA_SECURECONFIG

1 - 8 of 8

Custom Policies

☑	Policy Name
☑	UNAUTHORIZED_ACTIVITY_BY_EMP
☑	UNAUTHORIZED_ACTIVITY_BY_HR
☑	UNAUTHORIZED_ACTIVITY_BY_HRMGR

1 - 3 of 3

* Oracle recommends provisioning these policies.

- Single-click provisioning of core, predefined and custom policies
  - Core: Oracle recommended
  - Predefined: Out-of-the-box available in Oracle databases
  - Custom: User Defined

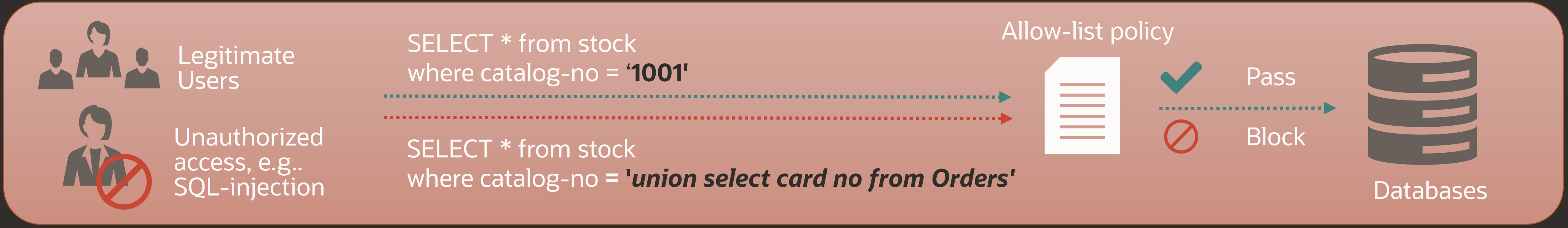
- Audit records are periodically collected from target and loaded into Audit Vault Server

Network-based SQL traffic monitoring

Network monitoring with database firewall

- Detection and blocking based on capturing normal application SQL patterns
- Detect or block never-before-seen SQL from reaching the database
- Anomaly detection and threat blocking with allow-list / deny-list based policy
- Does not use easy-to-defeat regular expressions

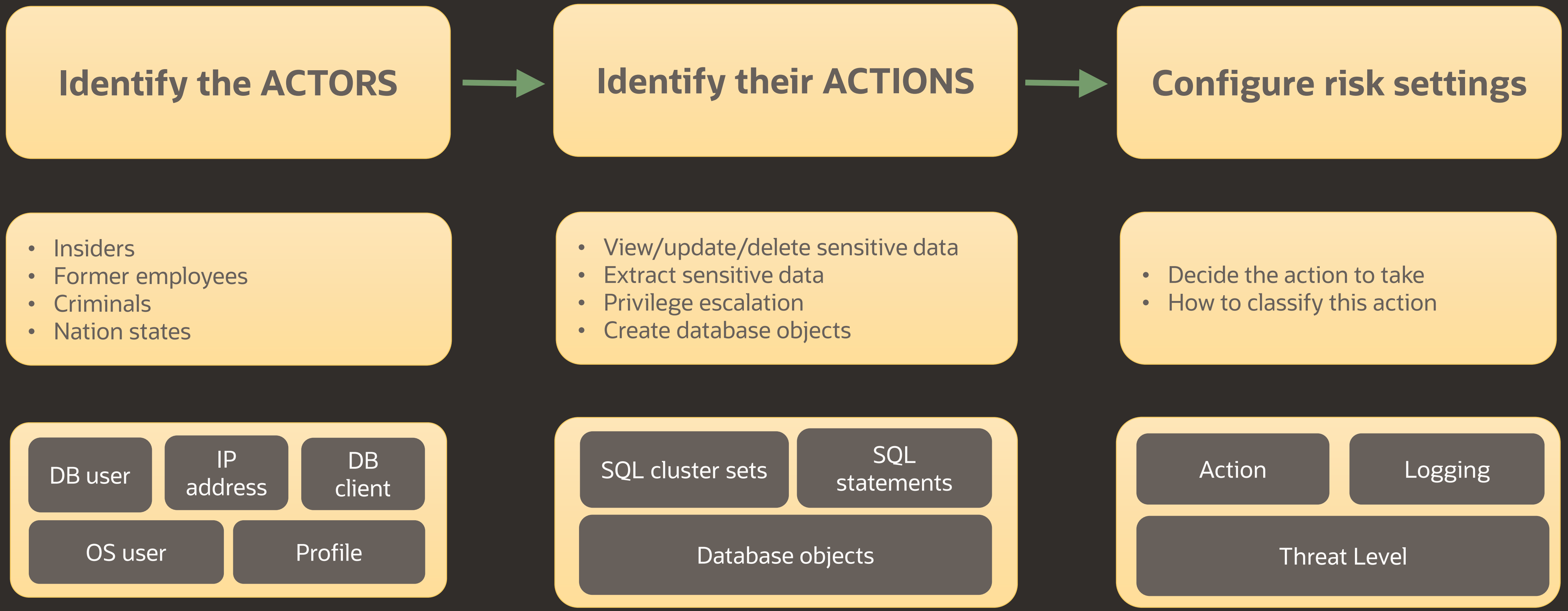
Allow-list based firewall policy



SELECT * from stock where catalog-no = ‘**1001'**

SELECT * from stock where catalog-no **= *'union select card no from Orders'***

Building policies in Database Firewall



Identify the ACTORS → Identify their ACTIONS → Configure risk settings

- Insiders
- Former employees
- Criminals
- Nation states

DB user | IP address | DB client | OS user | Profile

- View/update/delete sensitive data
- Extract sensitive data
- Privilege escalation
- Create database objects

SQL cluster sets | SQL statements | Database objects

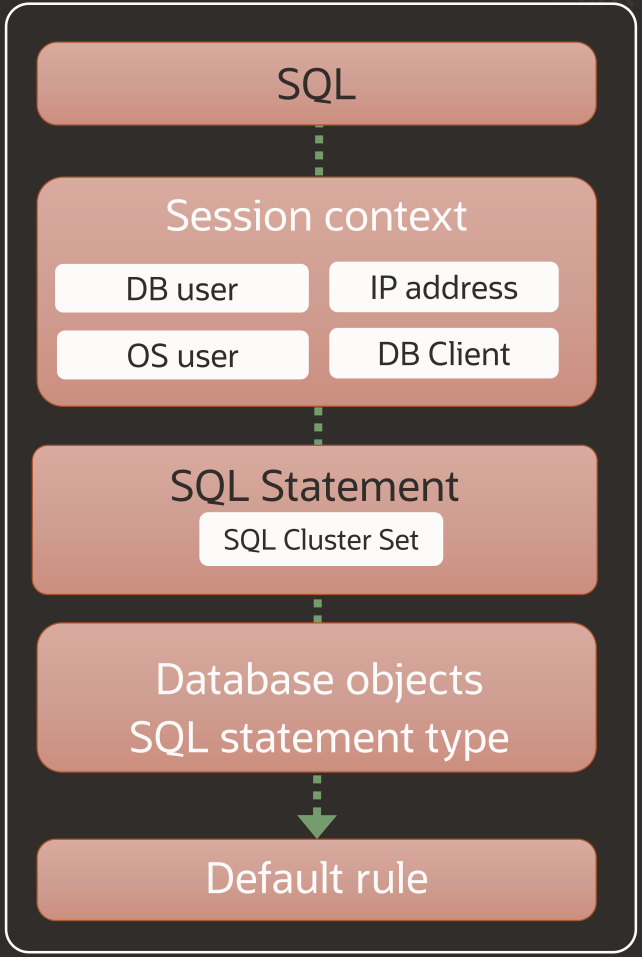
- Decide the action to take
- How to classify this action

Action | Logging | Threat Level

Multi-stage firewall

- Firewall policies can be based on session context, SQL Statement, database objects or a combination of them
- Policies execute in order as shown in the diagram
- Simple to complex firewall policies satisfying various use cases can be developed
- Simplified firewall configuration

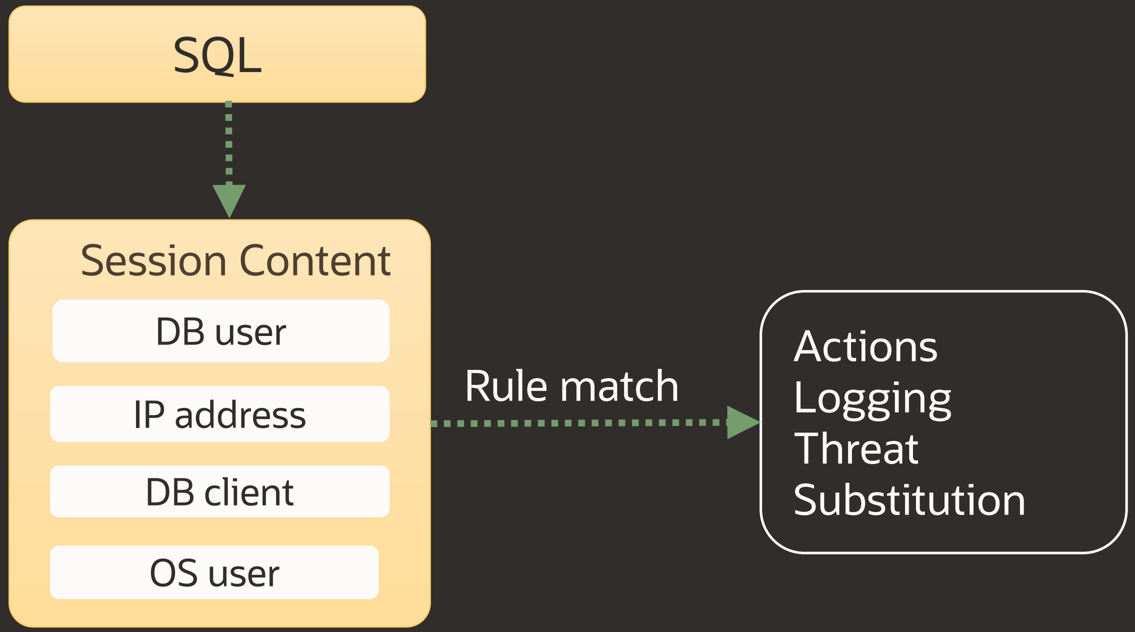
Order Of Execution



Implementing trusted application path using session context rules

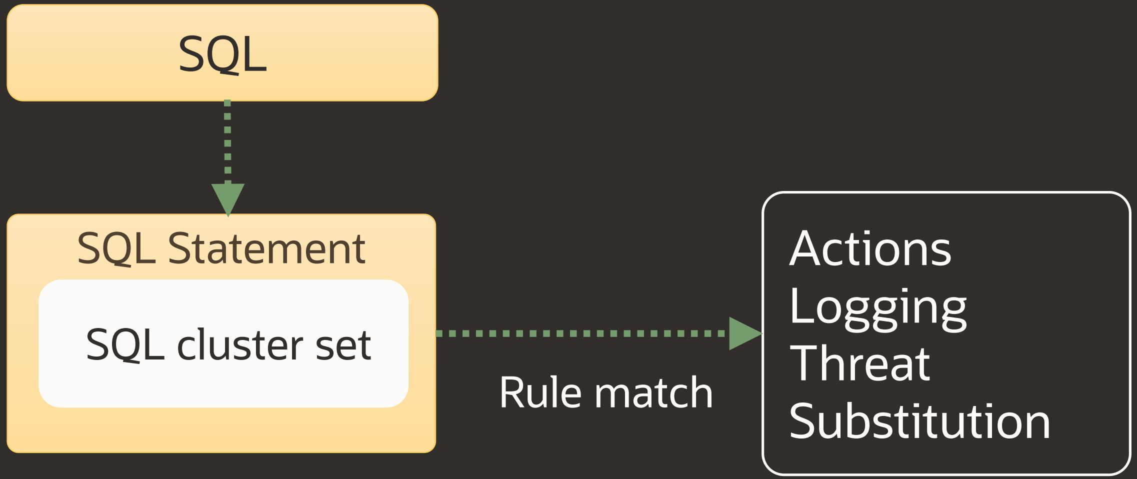
- Trusted application paths based on session attributes

- Use session content information to allow or block any statement, or log them, or alert



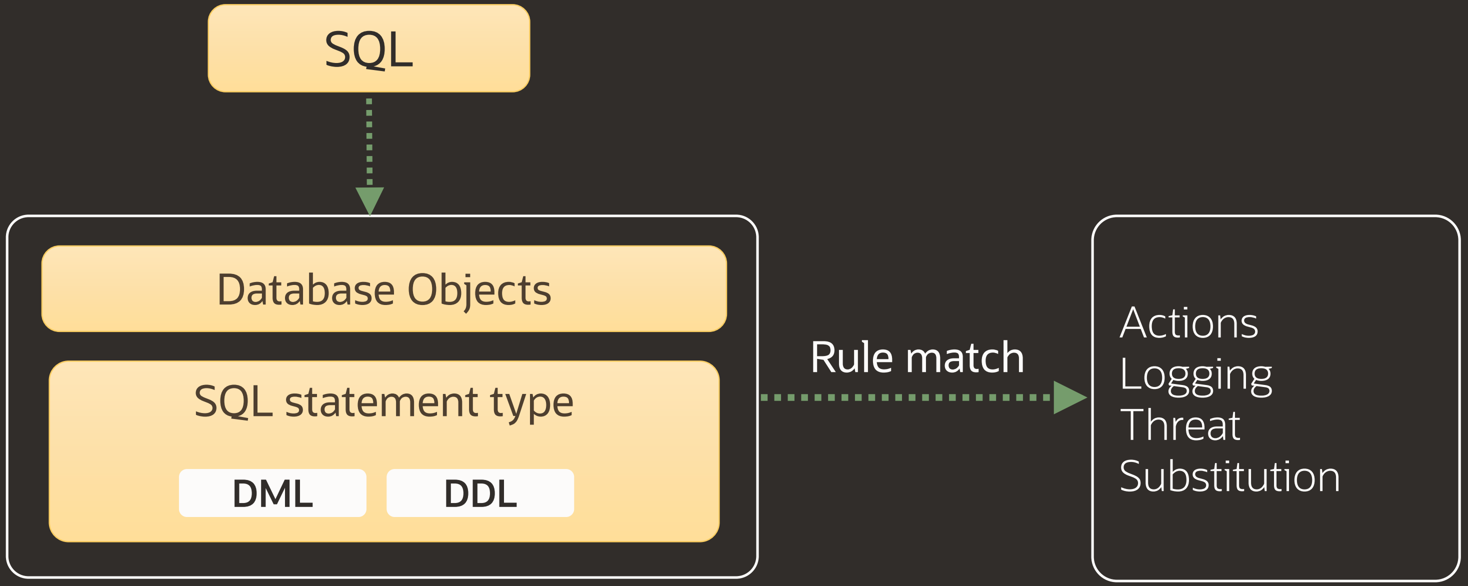
Analyzing SQL traffic to create allow-list/deny-list policies

- Train firewall based on known SQL to create allow-list or deny-list
- Implement policies based on specific SQL clusters – e.g. Privileged user access
  - Clusters are groups of SQL statements analyzed by Database Firewall to be similar



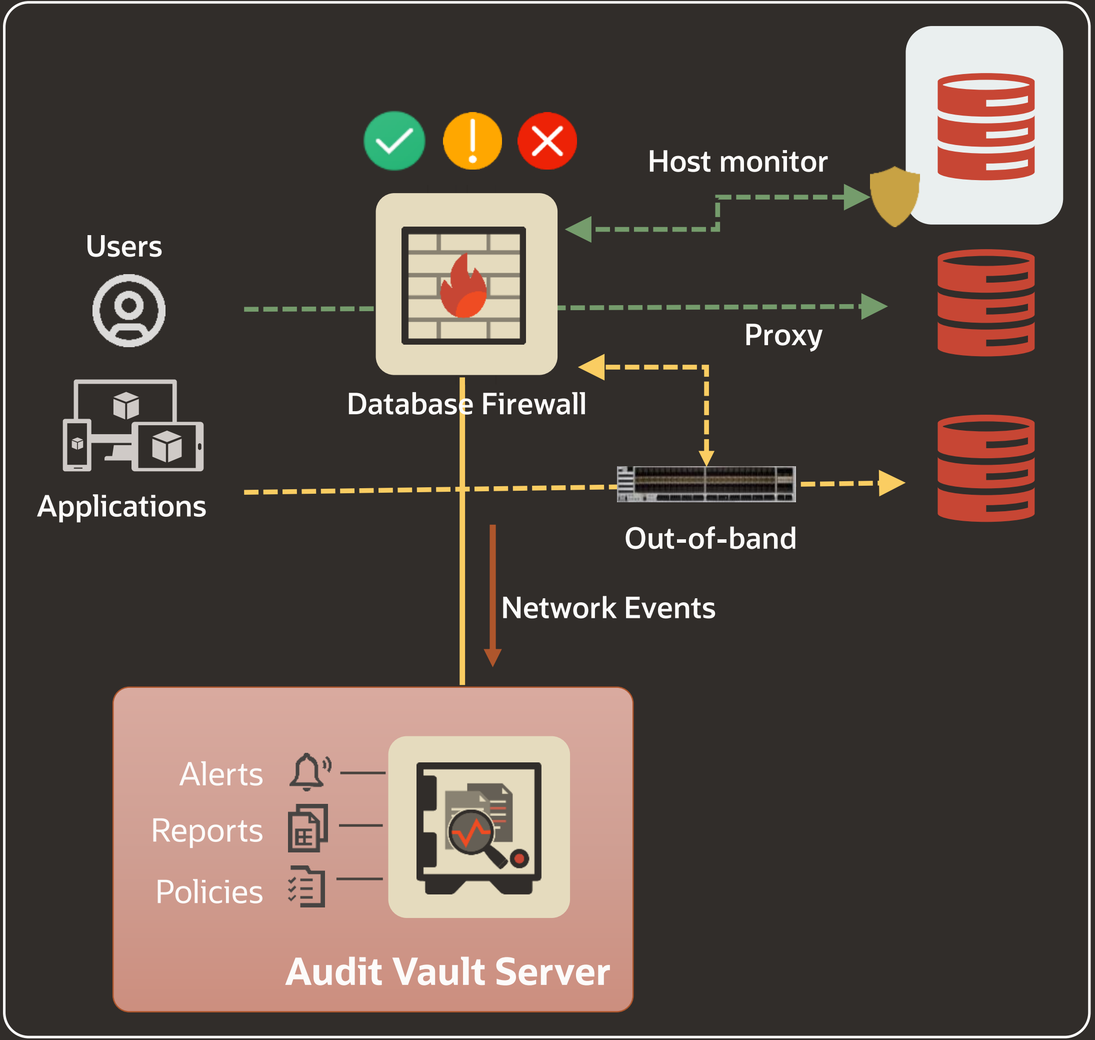
Creating policies specific to sensitive data and actions

- Create policies specific to sensitive tables and SQL operations
- Protect, monitor, alert on access to sensitive tables



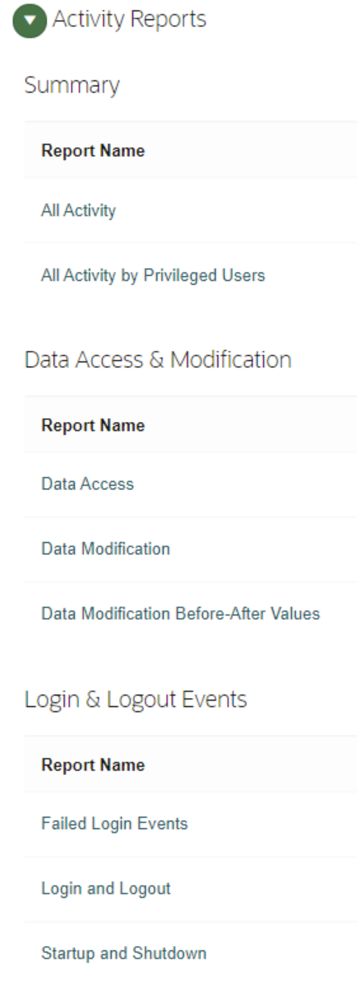
Firewall deployment modes

Mode	Details	Supported functionality	
		Monitoring	Blocking
Proxy	All client connections go via firewall, including return traffic	✓	✓
Host monitor	Agent running on database host listening to incoming traffic	✓	
Out-of-band	Monitors DB traffic sent to it (by span port, network taps, etc.)	✓	



Reporting and alerting

Rich set of out-of-the-box reports



Activity Reports

Summary

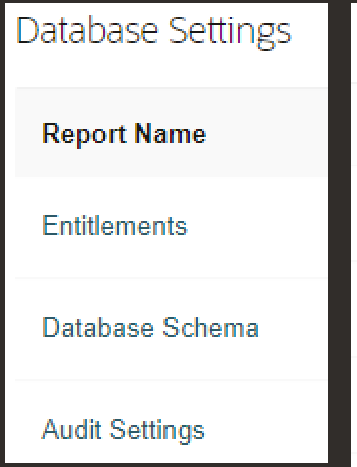
Report Name
All Activity
All Activity by Privileged Users

Data Access & Modification

Report Name
Data Access
Data Modification
Data Modification Before-After Values

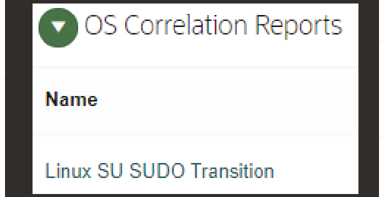
Login & Logout Events

Report Name
Failed Login Events
Login and Logout
Startup and Shutdown



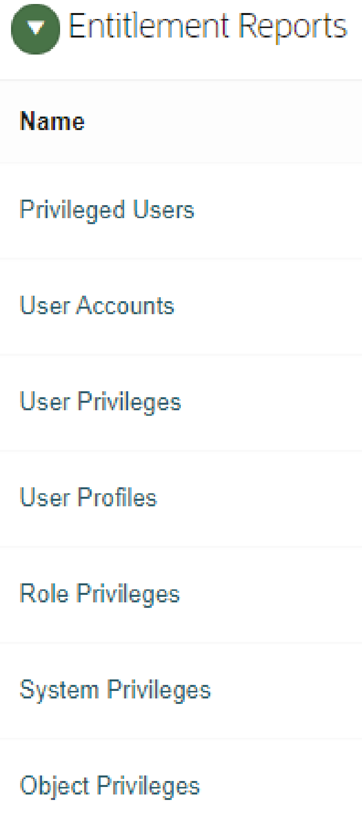
Database Settings

Report Name
Entitlements
Database Schema
Audit Settings



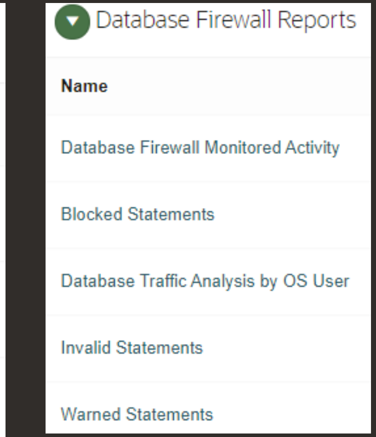
OS Correlation Reports

Name
Linux SU SUDO Transition



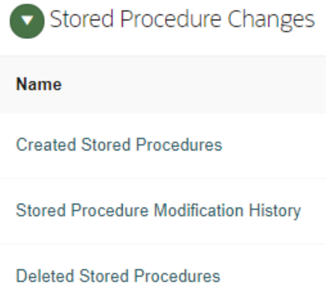
Entitlement Reports

Name
Privileged Users
User Accounts
User Privileges
User Profiles
Role Privileges
System Privileges
Object Privileges



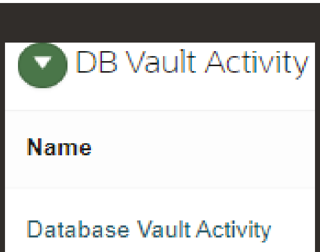
Database Firewall Reports

Name
Database Firewall Monitored Activity
Blocked Statements
Database Traffic Analysis by OS User
Invalid Statements
Warned Statements



Stored Procedure Changes

Name
Created Stored Procedures
Stored Procedure Modification History
Deleted Stored Procedures



DB Vault Activity

Name
Database Vault Activity

- Consolidated data from audit trail and firewall
- Customizable
- Can be scheduled and emailed
- Open schema allowing use of third-party tools for analysis

Many Reports for different Personas

Activity reports

Activity reports show all audit related database and firewall activities

Sensitive data access

Sensitive table list can be imported from Database Security Assessment Tool (DBSAT, Enterprise Manager)
Reports on sensitive tables, activity, access by privilege users, etc. is available

Entitlement changes

Entitlements can be retrieved on a scheduled or as-needed basis
Snapshots can be compared across time to see changes and discover privilege escalations

Anomaly detection and trend charts

Activity by newly seen or dormant IPs
Activity by newly created or dormant users

Database Firewall monitored activity

Analyze firewall activity, blocked statements, warned statements
Report below shows database firewall monitored activity

Compliance reports simplified

Compliance reports: GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, UK DPA

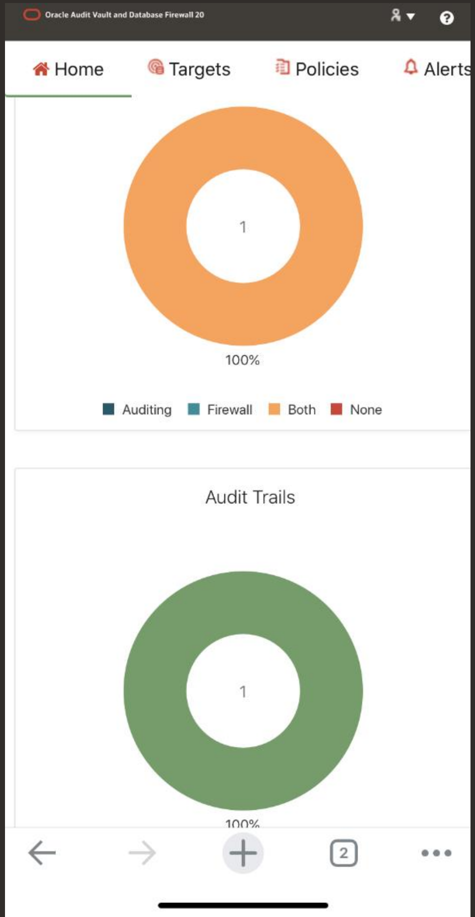
Alert policies

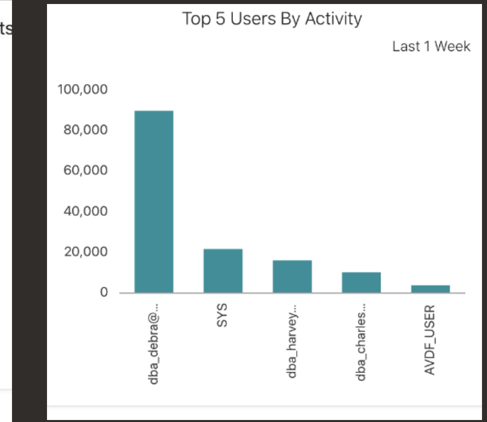
Alerts conditions based on audit record fields using SQL like expression
SQL like condition can be defined on one or more fields
Generated alerts can be viewed in “alert” reports, sent via email, and sent to syslog

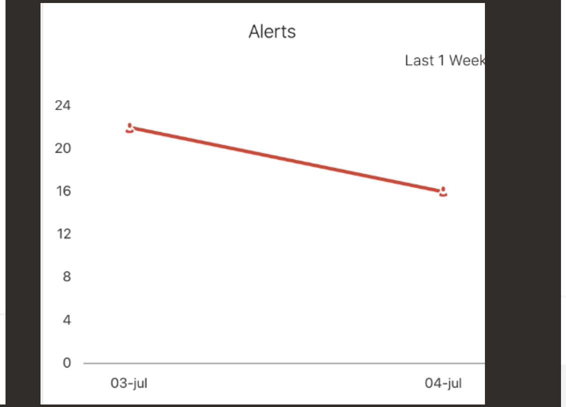
View AVDF on your mobile

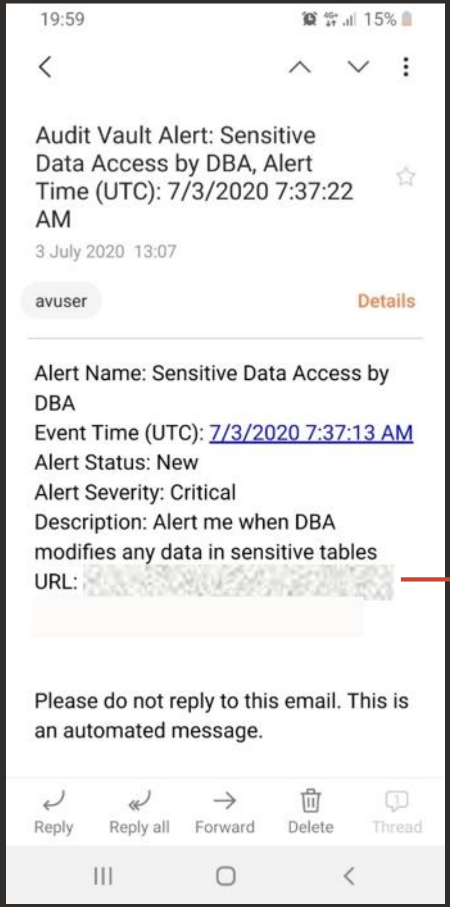
Dashboard

Alerts









Audit Vault Alert: Sensitive Data Access by DBA, Alert Time (UTC): 7/3/2020 7:37:22 AM

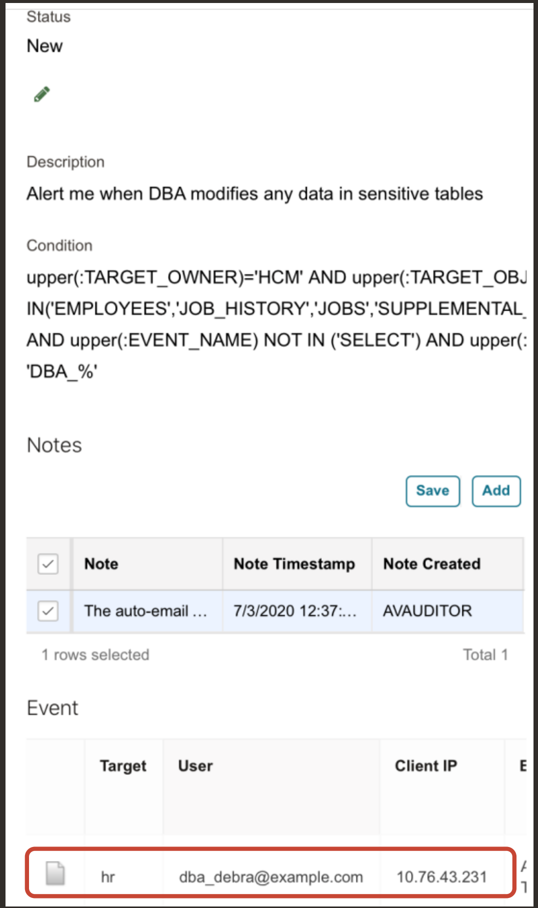
3 July 2020 13:07

avuser

Details

Alert Name: Sensitive Data Access by DBA
Event Time (UTC): 7/3/2020 7:37:13 AM
Alert Status: New
Alert Severity: Critical
Description: Alert me when DBA modifies any data in sensitive tables
URL: [redacted]

Please do not reply to this email. This is an automated message.



Status
New

Description
Alert me when DBA modifies any data in sensitive tables

Condition
upper(:TARGET_OWNER)='HCM' AND upper(:TARGET_OBJ
IN('EMPLOYEES','JOB_HISTORY','JOBS','SUPPLEMENTAL_
AND upper(:EVENT_NAME) NOT IN ('SELECT') AND upper(:
'DBA_%'

Notes

☑	Note	Note Timestamp	Note Created
☑	The auto-email ...	7/3/2020 12:37:...	AVAUDITOR

1 rows selected   Total 1

Event

	Target	User	Client IP	E
	hr	dba_debra@example.com	10.76.43.231	/ 1

ORACLE

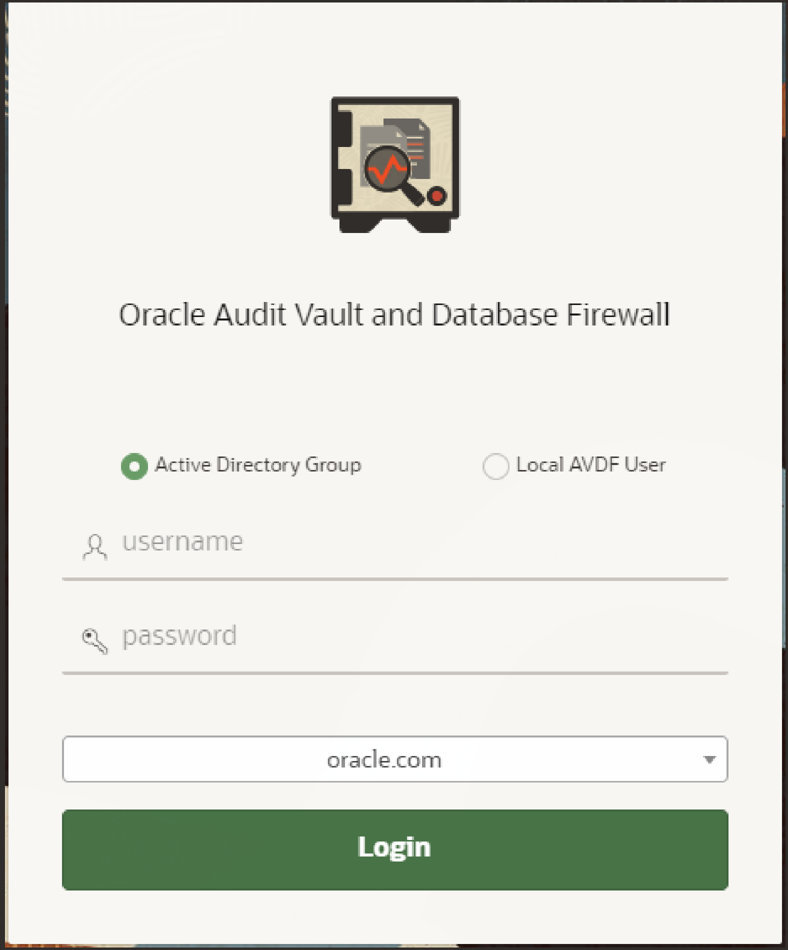
Enterprise deployment

Microsoft active directory / OpenLDAP integration

Supports user authentication and creation of new users

Logging into AVDF console

- Users (admins or auditors) can log into AVDF by selecting authentication mechanism to use
- Option 1: Login as AVDF user
- Option 2: Login as Active Directory or OpenLDAP user
  - Username, Password
  - Provide the group they belong to (to they are logged in as auditor or admin)



Oracle Audit Vault and Database Firewall

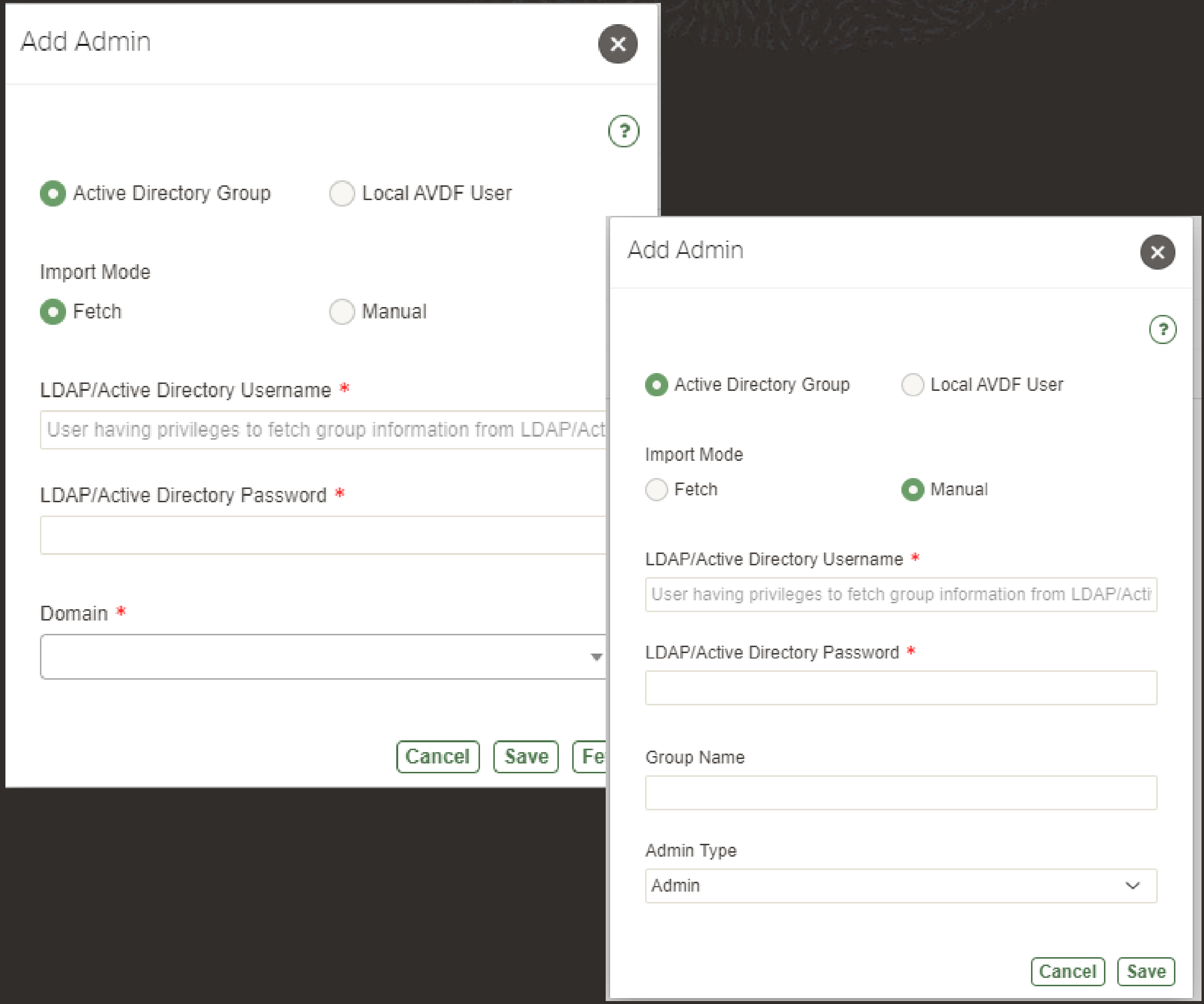
● Active Directory Group ○ Local AVDF User

Microsoft active directory / OpenLDAP integration

Supports user authentication and creation of new users

Creating new users

- New AVDF users (admins, auditors) can be created that exist only in AVDF, or are existing Active Directory/OpenLDAP users
- Option 1: AVDF user:
  - Username, password, admin type
- Option 2: Existing AD/OpenLDAP user:
  - User must exist before adding in AVDF
  - Select user from list of LDAP users and assign user type (admin, auditor etc.)



Add Admin

● Active Directory Group ○ Local AVDF User

Import Mode

● Fetch ○ Manual

LDAP/Active Directory Username *

User having privileges to fetch group information from LDAP/Act

LDAP/Active Directory Password *

Domain *

Add Admin

● Active Directory Group ○ Local AVDF User

Import Mode

○ Fetch ● Manual

LDAP/Active Directory Username *

User having privileges to fetch group information from LDAP/Acti

LDAP/Active Directory Password *

Group Name

Admin Type

Admin

SIEM/Syslog integration

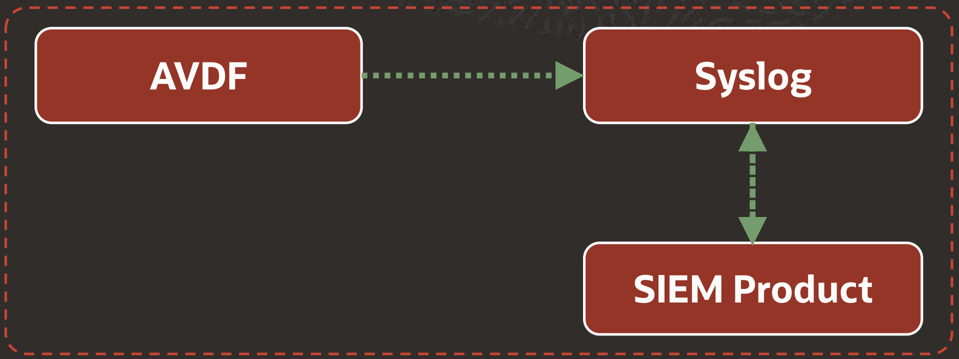
- AVDF alerts can be sent to syslog and integrated with SIEM product
  - Configure event fields to send
  - Forward alerts to syslog

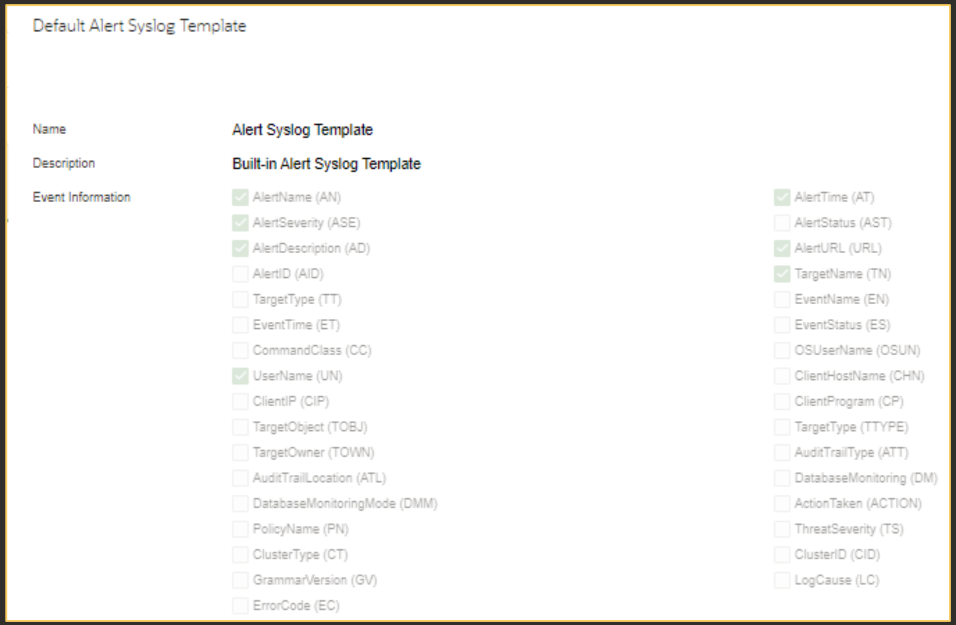
- SIEM products can also connect to audit vault server and read from the event log table

Alert Example in Syslog

```
AVDFAlert@111 name="Sensitive Data Access by DBA"
severity="Critical" url=“………" time="2020-07-
06T07:38:02.209875Z" target="hr"
user="dba_charles@example.com" desc="Alert me when DBA
modifies any data in sensitive tables”
```

Sending Alerts to Syslog




Default Alert Syslog Template

Name: Alert Syslog Template

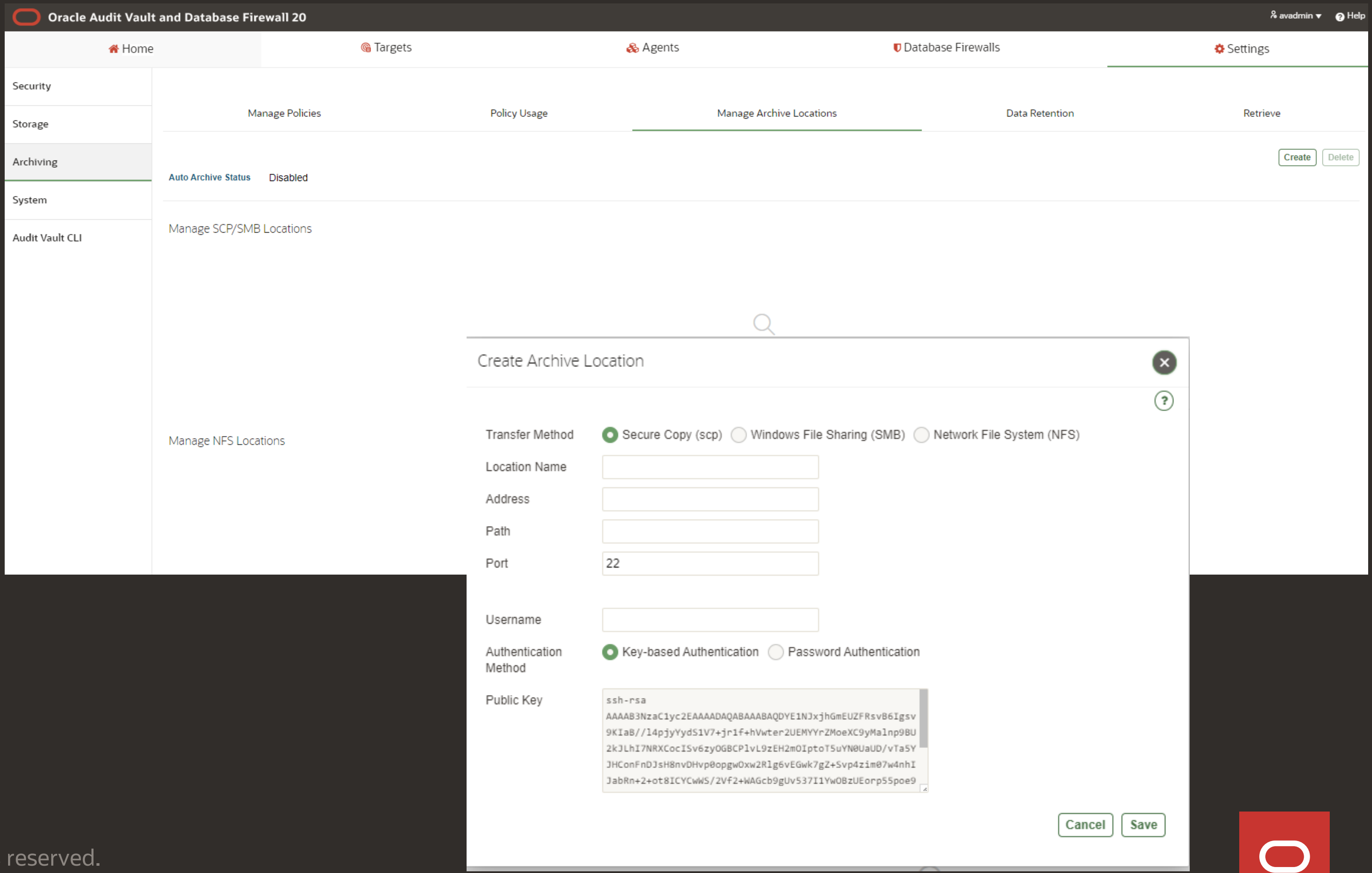
Description: Built-in Alert Syslog Template

Event Information

☑ AlertName (AN)
☑ AlertSeverity (ASE)
☑ AlertDescription (AD)
☐ AlertID (AID)
☐ TargetType (TT)
☐ EventTime (ET)
☐ CommandClass (CC)
☑ UserName (UN)
☐ ClientIP (CIP)
☐ TargetObject (TOBJ)
☐ TargetOwner (TOWN)
☐ AuditTrailLocation (ATL)
☐ DatabaseMonitoringMode (DMM)
☐ PolicyName (PN)
☐ ClusterType (CT)
☐ GrammarVersion (GV)
☐ ErrorCode (EC)
☑ AlertTime (AT)
☐ AlertStatus (AST)
☑ AlertURL (URL)
☑ TargetName (TN)
☐ EventName (EN)
☐ EventStatus (ES)
☐ OSUserName (OSUN)
☐ ClientHostName (CHN)
☐ ClientProgram (CP)
☐ TargetType (TTYPE)
☐ AuditTrailType (ATT)
☐ DatabaseMonitoring (DM)
☐ ActionTaken (ACTION)
☐ ThreatSeverity (TS)
☐ ClusterID (CID)
☐ LogCause (LC)

Audit data lifecycle management

- Per target archive policies can be created
  - Specify number of months online, archive
- Archived data can be retrieved by specifying from-to dates
- Support secure copy, windows file sharing, network file system
  - Nightly job moves data to archive



Auto Archive Status Disabled

Create Archive Location

Transfer Method ● Secure Copy (scp) ○ Windows File Sharing (SMB) ○ Network File System (NFS)

Location Name

Address

Path

Port 22

Username

Authentication Method ● Key-based Authentication ○ Password Authentication

Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDYE1NJxjhGmEUZFRsvB6Igsv
9KIaB//l4pjyYydS1V7+jr1f+hVwter2UEMYYrZMoeXC9yMalnp9BU
2kJLhI7NRXCocISv6zyOGBCPlvL9zEH2mOIptoT5uYN0UaUD/vTa5Y
JHConFnDJsH8nvDHvp0opgwOxw2Rlg6vEGwk7gZ+Svp4zim07w4nhI
JabRn+2+ot8ICYCwWS/2Vf2+WAGcb9gUv537I1YwOBzUEorp55poe9
```

High availability

Audit vault servers and database firewalls can be configured in HA

Audit and configuration data copied to secondary

Secondary becomes primary in the event of failover

Database firewall HA

Both primary, secondary receive same traffic in out-of-band and host monitor mode

- Database Firewalls have same configuration, synchronized by AV Server

In Proxy only one is active at a time

Supported targets and configurations

Supported targets

- Target types: database, operating system logs, directory system logs, file system logs
- Includes Oracle and non-Oracle targets
- Extensible for table and file-based trails

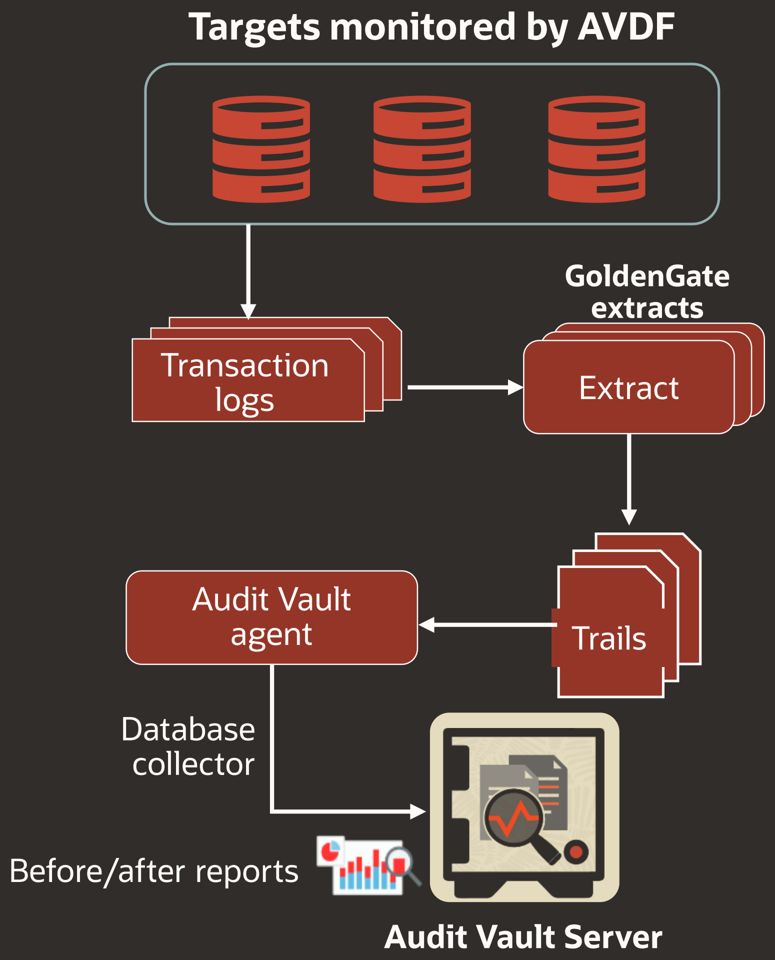
Databases
Oracle Database: on-prem, cloud (ATP-S, ADW-S), Exadata, RAC
IBM Db2: LUW, AIX
Microsoft SQL Server
SAP Sybase ASE
MySQL
PostgreSQL
MongoDB (via QuickJSON template)

Operating system logs
Oracle Solaris
Oracle Linux
Red Hat Enterprise Linux
Microsoft Windows Server
IBM AIX Power Systems
SuSE Linux

Directory service
Microsoft Active Directory

File system
Oracle ACFS

Before and after value capture using GoldenGate



- Install Oracle GoldenGate Microservices Architecture (min version 19.1.0.0.4)
- Configure Integrated Extract process in GoldenGate console for each source database
- Configure transaction log audit trail in AVDF
- Before/After values available in AVDF reports

Support for MongoDB (by configuring Quick JSON)

Support for MongoDB (by configuring Quick JSON)

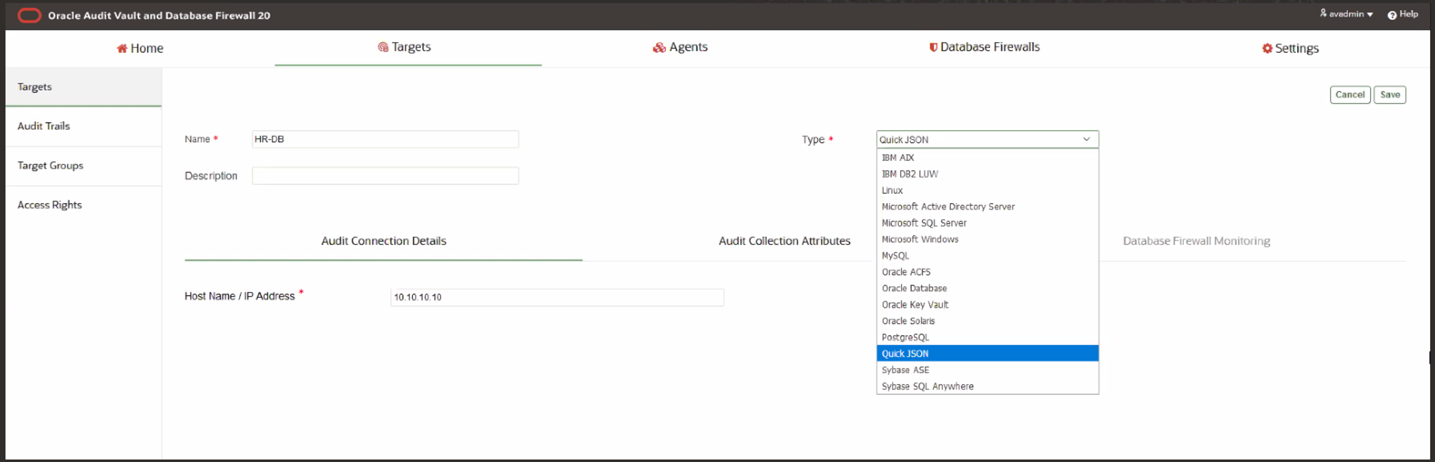
- Use Quick JSON as target type
- Provide collection attributes for fields in MongoDB audit trail

Add DIRECTORY Trail

- Provide location of directory trail
- Collector uses mapping to read from MongoDB audit trail and map to fields in Audit Vault Server

Mapping

- Provide the list of attributes and equivalent JSON file values
- Mapping provided in documentation



Name * HR-DB

Type * Quick JSON

Host Name / IP Address * 10.10.10.10

Audit Vault Collector Attribute	MongoDB JSON File Value
av.collector.qck.starttag	atype
av.collector.qck.eventtime	$.ts.$date
av.collector.qck.username	$.users[0].user
av.collector.qck.os.username	$.users[0].user
…	…

Support for JSON audit data (using Quick JSON)

Adding a Target

Use Quick JSON as target type

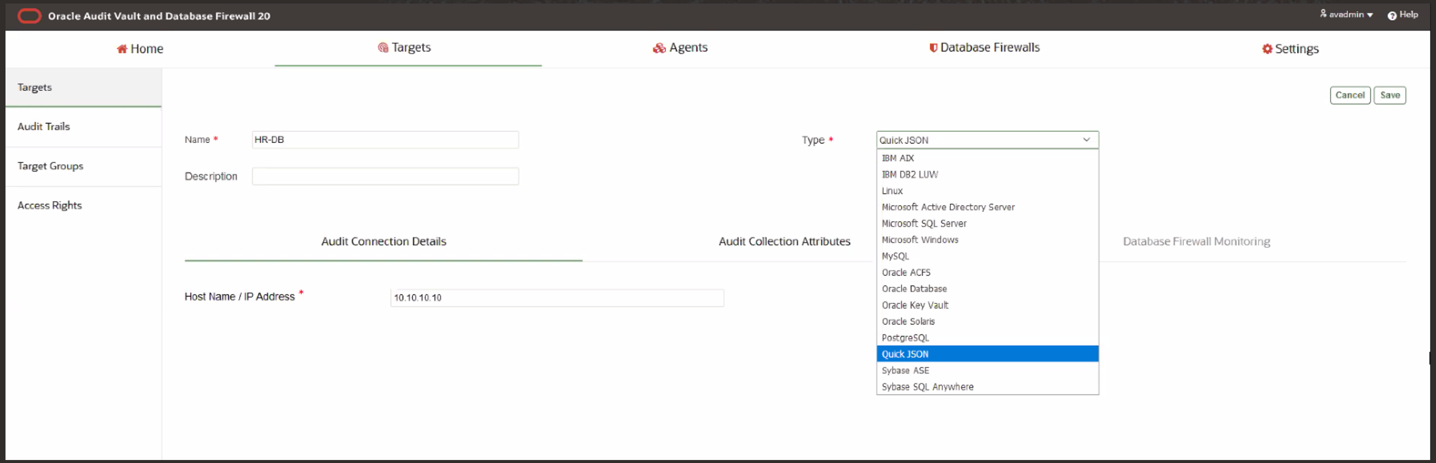
Provide collection attributes for fields

- Used to identify audit record fields in the JSON file

Adding DIRECTORY Trail

Provide location of directory trail

Collector uses mapping to read from JSON file and map to fields in Audit Vault Server

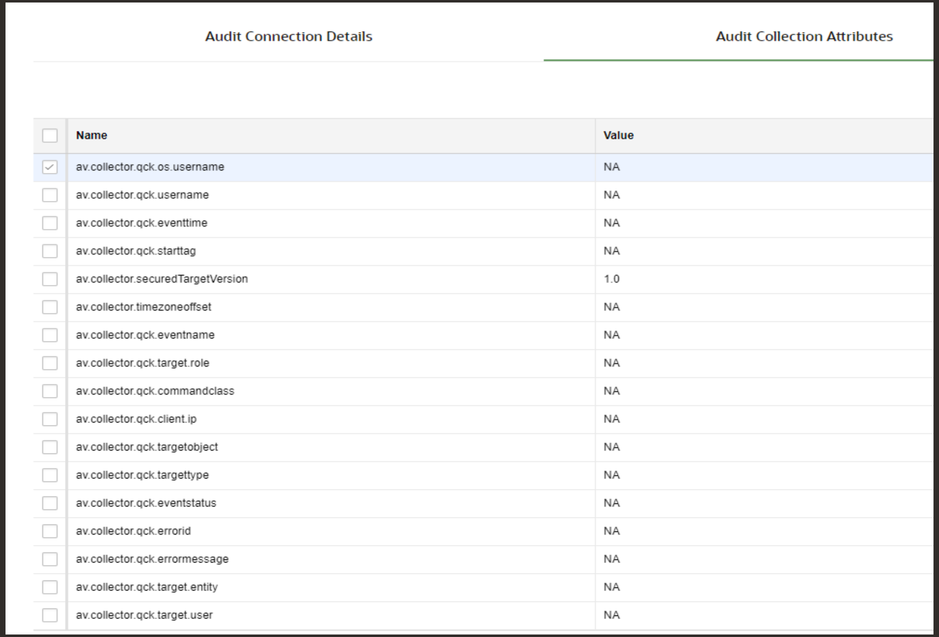


Name * HR-DB

Description

Type * Quick JSON

Host Name / IP Address * 10.10.10.10



	Name	Value
☑	av.collector.qck.os.username	NA
□	av.collector.qck.username	NA
□	av.collector.qck.eventtime	NA
□	av.collector.qck.starttag	NA
□	av.collector.securedTargetVersion	1.0
□	av.collector.timezoneoffset	NA
□	av.collector.qck.eventname	NA
□	av.collector.qck.target.role	NA
□	av.collector.qck.commandclass	NA
□	av.collector.qck.client.ip	NA
□	av.collector.qck.targetobject	NA
□	av.collector.qck.targettype	NA
□	av.collector.qck.eventstatus	NA
□	av.collector.qck.errorid	NA
□	av.collector.qck.errormessage	NA
□	av.collector.qck.target.entity	NA
□	av.collector.qck.target.user	NA

Collecting application audit data using extensible framework

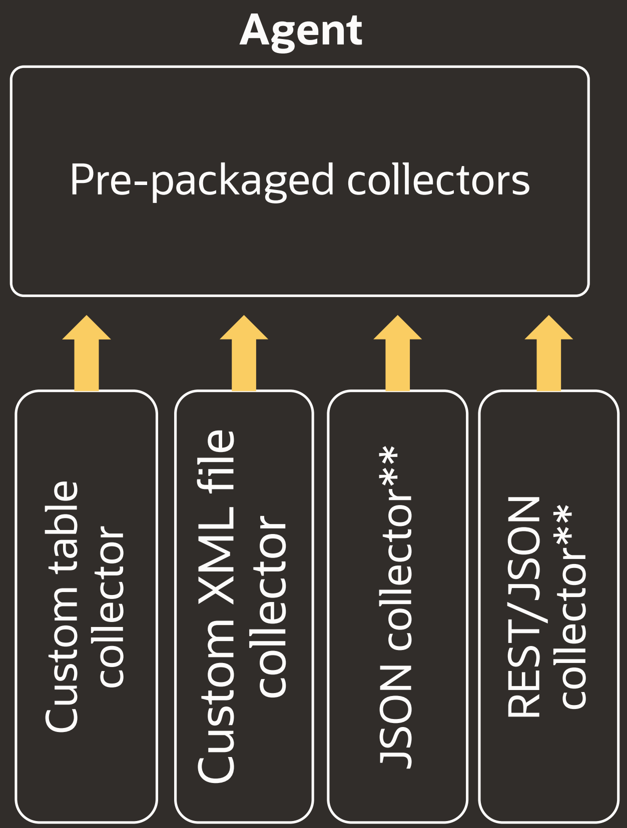
Extensible to add support for table, XML, REST, Quick JSON and JSON based trails. For more complex trail formats Java based collector can be written.

Similarly audit data in XML, JSON files can be collected, mapped to AVDF fields and stored

Application audit data stored in tables can be collected using “Custom table collector”

- Target audit record fields stored in tables can be mapped to corresponding AVDF fields using mapper file

Cloud audit trails can be supported using REST/JSON collector



**: New in AVDF 20

ORACLE

What’s new and summary

AVDF 20: What’s new

Expanded Audit Collection

- Built-in support for PostgreSQL
- Extending custom collector support to include JSON/REST, MongoDB
- Before/After values for Oracle databases

Simplified Database Firewall

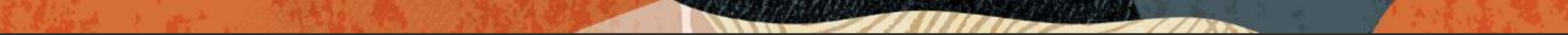
- Multi-stage firewall with simplified configuration
- Simpler policy creation using SQL cluster sets
- Oracle database RAC support
- NIC bonding for increased throughput
- SQL traffic collection on host machine on windows

Modernized User Interface

- Simplified navigation for common workflows
- Rich dashboards for auditors and admins
- Seeded audit policies for Oracle
- Unified console for audit and firewall management

Improved Enterprise Support

- LDAP/Active Directory authentication
- Automated archiving of audit/log data
- Multi-path Fiber Channel support for high availability



Summary

- Native database audit collection and SQL traffic monitoring
  - Audit collection from heterogeneous databases, OS logs with extensible custom collector framework
  - Database Firewall, enabling monitoring and blocking of suspicious SQL and preventing SQL injection
- Reporting and alerting with complex filtering to support forensic analysis
- Pre-build compliance reports: GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, UK DPA
- Enterprise features such as HA, ILM, SIEM/Syslog integration and LDAP authentication
- Hybrid cloud deployments supported

ORACLE