

IBM Security QRadar
7.4.1

Administration Guide



Note

Before you use this information and the product that it supports, read the information in [“Notices” on page 245](#).

Product information

This document applies to IBM® QRadar® Security Intelligence Platform 7.4.1 and subsequent releases unless superseded by an updated version of this document.

© **Copyright International Business Machines Corporation 2012, 2020.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction.....	ix
Chapter 1. What's new for administrators.....	1
New features and enhancements in QRadar 7.4.1.....	1
New features and enhancements in QRadar V7.4.0.....	3
Chapter 2. QRadar administration.....	7
Capabilities in your IBM QRadar product.....	7
Supported web browsers	8
Chapter 3. User management.....	11
Security profiles.....	11
Permission precedence.....	11
Creating a security profile.....	12
Editing a security profile.....	13
Duplicating a security profile.....	13
Deleting a security profile.....	14
Enterprise Federation authentication.....	14
Chapter 4. System management.....	15
System health information.....	15
QRadar component types.....	15
Data nodes.....	17
QRadar system time.....	17
NAT-enabled networks	18
Managed hosts.....	18
Bandwidth considerations for managed hosts.....	19
Encryption.....	19
Email servers.....	20
Configuration changes in your QRadar environment.....	21
Changes that impact event collection.....	22
Configuring an Event Collector.....	22
Deploying changes.....	23
Restarting the event collection service.....	24
Resetting SIM.....	24
Chapter 5. QRadar setup tasks.....	25
Network hierarchy.....	25
Guidelines for defining your network hierarchy.....	25
Acceptable CIDR values.....	26
Defining your network hierarchy.....	28
IF-MAP server certificates.....	29
Configuring IF-MAP Server Certificate for Basic Authentication.....	29
SSL certificates.....	29
SSL connections between QRadar components.....	30
IPv6 addressing in QRadar deployments.....	30
Advanced iptables rules examples.....	31
Configuring iptables rules.....	32
Data retention.....	33
Configuring retention buckets.....	34

Managing retention bucket sequence.....	35
Enabling and disabling a retention bucket.....	36
Deleting a Retention Bucket.....	36
System notifications.....	36
Configuring event and flow custom email notifications.....	37
Configuring custom offense email notifications.....	40
Custom offense close reasons.....	43
Adding a custom offense close reason.....	43
Editing custom offense close reason.....	43
Deleting a custom offense close reason.....	44
Configuring a custom asset property.....	44
Adding custom actions.....	44
Testing your custom action.....	45
Passing parameters to a custom action script.....	46
Managing aggregated data views.....	48
Chapter 6. Event data processing in QRadar.....	49
DSM Editor overview.....	49
Properties in the DSM Editor.....	50
Property configuration in the DSM Editor.....	51
Referencing capture strings by using format string fields.....	52
Regex for well-structured logs.....	52
Regex for natural language logs.....	53
Expressions in JSON format for structured data.....	53
JSON keypath expressions.....	54
Expressions in LEEF format for structured data.....	56
Expressions in CEF format for structured data.....	57
Expressions in Name Value Pair format for structured data.....	58
Expressions in Generic List format for structured data.....	58
Expressions in XML format for structured data.....	58
Opening the DSM Editor.....	59
Configuring a log source type.....	59
Configuring property autodetection for log source types.....	60
Configuring Log Source Autodetection for Log Source types.....	60
Configuring DSM parameters for Log Source types.....	62
Custom log source types.....	62
Creating a custom log source type to parse events.....	63
Custom property definitions in the DSM Editor.....	64
Selectivity.....	64
Expressions.....	64
Creating a custom property.....	64
Event mapping.....	67
Creating an event map and categorization.....	67
Chapter 7. Using reference data in QRadar.....	69
Types of reference data collections.....	69
Reference sets overview.....	70
Adding, editing, and deleting reference sets.....	71
Viewing the contents of a reference set.....	72
Adding elements to a reference set.....	73
Exporting elements from a reference set.....	74
Deleting elements from a reference set.....	74
Creating reference data collections with the APIs.....	75
Reference data collection examples.....	77
Tracking expired user accounts.....	77
Integrate dynamic data from external sources	78

Chapter 8. User information source configuration.....	79
User information source overview.....	79
User information sources.....	79
Reference data collections for user information.....	80
Integration workflow example.....	80
Chapter 9. IBM X-Force integration.....	83
X-Force Threat Intelligence feed	83
X-Force data on the dashboard.....	83
IBM QRadar Security Threat Monitoring Content Extension app.....	84
Installing the IBM QRadar Security Threat Monitoring Content Extension application.....	84
IBM X-Force Exchange plug-in for QRadar.....	85
Chapter 10. Flow sources.....	87
Types of flow sources.....	88
NetFlow.....	88
IPFIX.....	89
sFlow.....	91
J-Flow.....	91
Packeteer.....	92
Flowlog file.....	92
Napatech interface.....	92
Adding or editing a flow source.....	92
Enabling and disabling a flow source.....	93
Deleting a Flow Source.....	93
Flow source aliases.....	93
Adding a flow source alias.....	94
Deleting a flow source alias.....	94
Correcting flow time stamps.....	94
Chapter 11. Remote networks and services configuration.....	97
Default remote network groups.....	97
Default remote service groups.....	98
Guidelines for network resources.....	99
Managing remote networks objects.....	99
Managing remote services objects.....	100
Chapter 12. Server discovery.....	101
Discovering servers.....	101
Chapter 13. Domain segmentation.....	103
Overlapping IP addresses.....	103
Domain definition and tagging.....	104
Creating domains.....	107
Creating domains for VLAN flows.....	108
Domain privileges that are derived from security profiles.....	109
Domain-specific rules and offenses.....	111
Example: Domain privilege assignments based on custom properties.....	113
Chapter 14. Multitenant management.....	115
User roles.....	115
Domains and log sources.....	116
Provisioning a new tenant.....	117
Monitoring license usage.....	117
Rules management in multitenant deployments.....	118

Network hierarchy updates in a multitenant deployment.....	119
Chapter 15. Asset Management.....	121
Sources of asset data.....	121
Incoming asset data workflow.....	123
Updates to asset data.....	125
Asset reconciliation exclusion rules.....	125
Asset merging.....	126
Identification of asset growth deviations.....	127
System notifications that indicate asset growth deviations.....	127
Example: How configuration errors for log source extensions can cause asset growth deviations.....	128
Troubleshooting asset profiles that exceed the normal size threshold.....	128
New asset data is added to the asset blacklists.....	129
Prevention of asset growth deviations.....	129
Stale asset data.....	130
Asset blacklists and whitelists.....	130
Identity exclusion searches.....	133
Advanced tuning of asset reconciliation exclusion rules.....	133
Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist.....	135
Clean up asset data after growth deviations.....	135
Deleting blacklist entries.....	136
Chapter 16. Event store and forward	137
Chapter 17. Security content.....	139
Types of security content.....	139
Methods of importing and exporting content.....	140
Installing extensions by using Extensions Management.....	140
Uninstalling a content extension.....	141
Content type identifiers for exporting custom content.....	142
Chapter 18. SNMP trap configuration.....	145
Chapter 19. Sensitive data protection.....	147
How does data obfuscation work?.....	147
Data obfuscation profiles.....	148
Data obfuscation expressions.....	148
Scenario: Obfuscating user names.....	149
Creating a data obfuscation profile.....	150
Creating data obfuscation expressions.....	150
Deobfuscating data so that it can be viewed in the console.....	151
Chapter 20. Event categories.....	153
High-level event categories.....	153
Recon.....	154
DoS.....	156
Authentication.....	159
Access.....	168
Exploit.....	170
Malware.....	172
Suspicious Activity.....	173
System.....	178
Policy.....	183
Unknown.....	185
CRE.....	186
Potential Exploit.....	186

Flow.....	187
User Defined.....	189
SIM Audit.....	192
VIS Host Discovery.....	193
Application.....	193
Audit.....	219
Control.....	223
Asset Profiler.....	225
Sense.....	230
Chapter 21. Common ports and servers used by QRadar.....	233
QRadar port usage	233
QRadar public servers.....	241
Chapter 22. RESTful API	243
Accessing the interactive API documentation page.....	243
Notices.....	245
Trademarks.....	246
Terms and conditions for product documentation.....	246
IBM Online Privacy Statement.....	247
General Data Protection Regulation.....	247
Glossary.....	249
A.....	249
B.....	249
C.....	250
D.....	250
E.....	251
F.....	251
G.....	251
H.....	251
I.....	252
K.....	252
L.....	252
M.....	253
N.....	253
O.....	254
P.....	254
Q.....	254
R.....	254
S.....	255
T.....	256
V.....	256
W.....	256
Index.....	257

Introduction to QRadar product administration

Administrators use IBM QRadar SIEM to manage dashboards, offenses, log activity, network activity, assets, and reports.

Intended audience

This guide is intended for all QRadar SIEM users responsible for investigating and managing network security. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

Technical documentation

To find IBM QRadar product documentation on the web, including all translated documentation, access the [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>).

For information about how to access more technical documentation in the QRadar products library, see [Accessing IBM Security Documentation Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the [Support and Download Technical Note](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar.

Chapter 1. What's new for administrators

Learn about the new features and capabilities that make it easier for you to configure and administer your IBM QRadar deployment.

New features and enhancements in QRadar 7.4.1

The following new features and enhancements make it easier for administrators to manage their IBM QRadar 7.4.1 deployment.

To view a list of all new features in this release, see the *What's New* document on the [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html) (www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html).

Parsing status in the DSM Editor

In the **Log Activity Preview** of the DSM Editor, you can track the status of event properties. The **Parsing Status** column indicates whether your event properties are successfully parsing and mapping to a QID record.


The following figure shows how the parsing status is displayed.

Figure 1. Parsing Status for event properties

Log Activity Preview (Parsing Failed:1/58 -- Parsed but NOT Mapped:56/58)

A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Parsing Status*	Destination IP	Destination MAC	Destination Port	Event Category	Event ID	Event Name
Parsing Failed	0.0.0.0			3Com 8800 Series Switch		unknown
Parsed and Mapped	0.0.0.0			3Com 8800 Series Switch	test dat n5 CEF	CMD
Parsed but NOT Mapped	0.0.0.0			3Com 8800 Series Switch	test dat n6 CEF	unknown
Parsed but NOT Mapped	0.0.0.0			3Com 8800 Series Switch	test dat n CEF	unknown

 [Learn more about the Log Activity Preview...](#)

Support for multiline event payloads in the DSM Editor

In the DSM Editor, you can specify a custom delimiter that makes it easier for QRadar 7.4.1 to ingest multiline events. To ensure that your event is kept intact as a single multiline event, select the **Override event delimiter** checkbox to separate the individual events based on another character or sequence of characters. For example, if your configuration is ingesting multiline events, you can add a special character to the end of each distinct event in the **Workspace**, and then identify this special character as the event delimiter.

The following figures show how you can use the **Override event delimiter** checkbox to specify double exclamation marks as the custom delimiter for a payload.

Workspace

Use sample event payloads to help fine tune the behavior of this Log Source Type. Matches in the payload are highlighted when a property is selected. Note: System properties that have not been overridden cannot be highlighted in the workspace.

☒ Wrap Content

☐ Override event delimiter 

```
1 | <13>Feb 02 12:17:03 microsoft.windows.test.com AgentDevice=WindowsLog AgentLog
File=Security Source=Security Computer=BCDC01 User=SYSTEM Domain= EventID=672 Ev
entIDCode=672 EventType=8 !!EventCategory=9 RecordNumber=74685994 TimeGenerate
d=1233605821 TimeWritten=1233605821 Message=Authentication Ticket Request: User Name:
BCVMLIC01$ Supplied Realm Name: RADISYS.COM User ID: %{S-1-5-21-1456488807-1979357023-3472
770521-11000} Service Name: krbtgt Service ID: %{S-1-5-21-1456488807-1979357023-3472770521
-502} Ticket Options: 0x10 Result Code: - Ticket Encryption Type: 0x17 Pre-Authentication
Type: 2 Client Address: 172.20.100.16 Certificate Issuer Name: Certificate Serial Number:
Certificate Thumbprint:
2 | <13>Feb 02 12:15:57 microsoft.windows.test.com AgentDevice=WindowsLog AgentLogFi
le=Security Source=Security Computer=ORDC01 User=SYSTEM Domain= EventID=672 Ev
entIDCode=672 EventType=8 EventCategory=9 RecordNumber=1091884495 TimeGenerated=1233
605756 TimeWritten=1233605756 Message=Authentication Ticket Request: User Name: LAB-PC-A
$ Supplied Realm Name: RADISYS.COM User ID: %{S-1-5-21-1456488807-1979357023-3472770521-16
742} Service Name: krbtgt Service ID: %{S-1-5-21-1456488807-1979357023-3472770521-502} Tic
ket Options: 0x40810010 Result Code: - Ticket Encryption Type: 0x17 Pre-Authentication Type: 2
```

Figure 2. Payload without a specified custom event delimiter

Workspace

Use sample event payloads to help fine tune the behavior of this Log Source Type. Matches in the payload are highlighted when a property is selected. Note: System properties that have not been overridden cannot be highlighted in the workspace.

☒ Wrap Content

☒ Override event delimiter 

```
1 | <13>Feb 02 12:17:03 microsoft.windows.test.com AgentDevice=WindowsLog
AgentLogFile=Security Source=Security Computer=BCDC01 User=SYSTEM Domain= EventID=67
2
EventIDCode=672 EventType=8
EventCategory=9 RecordNumber=74685994 TimeGenerated=1233605821 TimeWritten=1233605821 Me
ssage=Authentication Ticket Request: User Name: BCVMLIC01$ Supplied Realm Name: RADISYS.CO
M User ID: %{S-1-5-21-1456488807-1979357023-3472770521-11000} Service Name: krbtgt Service
ID: %{S-1-5-21-1456488807-1979357023-3472770521-502} Ticket Options: 0x10 Result Code: - T
icket Encryption Type: 0x17 Pre-Authentication Type: 2 Client Address: 172.20.100.16 Certi
ficate Issuer Name: Certificate Serial Number: Certificate Thumbprint:
2 | <13>Feb 02 12:15:57 microsoft.windows.test.com AgentDevice=WindowsLog AgentLogFi
le=Security Source=Security Computer=ORDC01 User=SYSTEM Domain= EventID=672 Ev
entIDCode=672 EventType=8 EventCategory=9 RecordNumber=1091884495 TimeGenerated=1233
605756 TimeWritten=1233605756 Message=Authentication Ticket Request: User Name: LAB-PC-A
$ Supplied Realm Name: RADISYS.COM User ID: %{S-1-5-21-1456488807-1979357023-3472770521-16
742} Service Name: krbtgt Service ID: %{S-1-5-21-1456488807-1979357023-3472770521-502} Tic
ket Options: 0x40810010 Result Code: - Ticket Encryption Type: 0x17 Pre-Authentication Type: 2
```

Figure 3. Payload with a specified custom event delimiter

 [Learn more about the DSM Editor Workspace...](#)

Event ID and Event Category fields copied to Event Mapping

In QRadar 7.4.1, you can select the unmapped **Event ID** and **Event Category** fields of your previewed events to copy them into the corresponding event mapping fields. Now you can map your events to QID records faster than in previous versions, where you had to manually enter your event ID and event category combinations to create your event mappings. On the **Event Mappings** tab, go to the **Unknown Event Mappings** section of the **Create a New Event Mapping** window. Click on a row to copy the event ID and the event category into the corresponding fields, and then click **Create**.

The following figure shows how you can create new event mappings in the **Event Mappings** tab of the DSM Editor.

Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

Unknown Event Mappings
This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

Event ID	Event Category
test dat n5 CEF	3Com 8800 Series Switch
test dat n6 CEF	3Com 8800 Series Switch
test dat n CEF	3Com 8800 Series Switch
test dat n4 CEF	3Com 8800 Series Switch


Event ID
test dat n4 CEF

Event Category
3Com 8800 Series Switch

QID Record
[Choose QID...](#)

Create **Close**

Figure 4. Create a new event mapping

 [Learn more about event mappings...](#)

New features and enhancements in QRadar V7.4.0

The following new features and enhancements make it easier for administrators to manage their IBM QRadar V7.4.0 deployment.

To view a list of all new features in this release, see the *What's New* document on the IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SS42VS_7.4.0/com.ibm.qradar.doc/c_pdf_launch.html).

Global System Notifications configuration

Global System Notifications are now local, making them host specific and more useful. As a result, the thresholds are now set automatically by QRadar and the Global System Notification section of the Admin tab was removed.

Secure email server

Send email to distribute alerts, reports, notifications, and event messages to mail servers that require authentication.

You can configure an email server for your entire QRadar deployment, or multiple email servers.

 [Learn more about configuring Secure email server...](#)

DSM Parameter support in the DSM Editor

In QRadar 7.4.0, if your log source type has DSM parameters, you can use the DSM Editor to configure the DSM parameters. Enable the **Display DSM Parameters Configuration** option to view and edit the DSM parameters.

Juniper Steel-Belted Radius**Change**

Properties

Event Mappings

Configuration**DSM Parameters Configuration****Display DSM Parameters Configuration**

If there are any DSM Parameters for this log source type, enable this option to view and edit those DSM Parameters.

**Event Collector**

Default

The Default parameter set applies to all instances of this DSM in the deployment which do not have an Event Collector-specific override. To set different parameter values for this DSM for a specific Event Collector select it from the list and override the Default settings.

User Field

User-Name

Customize JunipserSBR DSM to fields mapping

Full Name Field

Full-Name

Customize JunipserSBR DSM to fields mapping

Source IP Field

Source-IP-Add

Customize JunipserSBR DSM to fields mapping

Source Port Field

Source-UDP-F

Customize JunipserSBR DSM to fields mapping

Destination IP Field

Customize JunipserSBR DSM to fields mapping

Destination Port Field

Target-UDP-Pc

Customize JunipserSBR DSM to fields mapping

[Learn more about configuring DSM parameters in the DSM Editor...](#)

Reverse tunnel initiation

The SSH tunnel between two managed hosts can now be initiated from the remote host instead of the local host. For example, you have a connection from an Event Processor in a secure environment to an Event Collector that is outside of the secure environment. You also have a firewall rule that prevents you from having a host outside the secure environment connect to a host in the secure environment. In QRadar 7.4.0, you can switch which host creates the tunnel so that the connection is established from the Event Processor by selecting the Remote Tunnel Initiation checkbox for the Event Collector.

[Learn more about reverse tunnel initiation...](#)


Improved flow timestamp handling

Two new configuration settings provide more control over the way that flow timestamps are handled when Netflow V9 begins sending records with overflowed system uptime values. The new settings eliminate the need to reset the first and last switched times.

The new configuration options and the default values are shown here:

- `NORMALISE_OVERFLOWED_UPTIMES=YES`
- `UPTIME_OVERFLOW_THRESHOLD_MSEC=86400000`

The timestamps are corrected when the system uptime value is less than the first and last switched packet times by more than the value that is specified in the `UPTIME_OVERFLOW_THRESHOLD_MSEC` configuration. The timestamps are corrected based on the assumption that the system uptime wrapped around the maximum 32-bit value.

 [Learn more about managing flow timestamps...](#)

Chapter 2. QRadar administration

As an IBM QRadar administrator, you have a variety of tools available to help you configure and manage your QRadar deployment.

For example, using the tools on the **Admin** tab, you can perform the following tasks:

- Deploy and manage QRadar hosts and licenses.
- Configure user accounts and authentication.
- Build a network hierarchy.
- Configure domains and set up a multi-tenant environment.
- Define and manage log and flow data sources.
- Manage QRadar data retention.
- Manage assets and reference data.
- Schedule regular backups of QRadar configuration and data.
- Monitor the system health of managed hosts.

Capabilities in your IBM QRadar product

IBM QRadar product documentation describes functionality such as offenses, flows, assets, and historical correlation, that might not be available in all QRadar products. Depending on the product that you are using, some documented features might not be available in your deployment.

IBM QRadar Log Manager

QRadar Log Manager is a basic, high-performance, and scalable solution for collecting, analyzing, storing, and reporting on large volumes of network and security event logs.

IBM QRadar SIEM

QRadar SIEM is an advanced offering that includes the full range of security intelligence capabilities for on-premises deployments. It consolidates log source and network flow data from thousands of assets, devices, endpoints, and applications that are distributed throughout your network, and performs immediate normalization and correlation activities on the raw data to distinguish real threats from false positives.

IBM QRadar on Cloud

QRadar on Cloud provides IBM security professionals to manage the infrastructure, while your security analysts perform the threat detection and management tasks. You can protect your network, and meet compliance monitoring and reporting requirements, with reduced total cost of ownership.

QRadar product capabilities

Review the following table to compare the capabilities in each QRadar product.

Table 1. Comparison of QRadar capabilities			
Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Full administrative capabilities	Yes	No	Yes
Supports hosted deployments	No	Yes	No
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes

Table 1. Comparison of QRadar capabilities (continued)			
Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand-alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
Network activity monitoring	Yes	Yes	No
Asset profiling	Yes	Yes	No ¹
Offenses management	Yes	Yes	No
Network flow capture and analysis	Yes	Yes	No
Historical correlation	Yes	Yes	No
QRadar Network Insights integration	Yes	Yes	No
QRadar Vulnerability Manager integration	Yes	Yes	Yes
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No
Vulnerability assessment scanners	Yes	Yes	Yes
¹ QRadar Log Manager tracks asset data only if QRadar Vulnerability Manager is installed.			

Some documentation, such as the *Administration Guide* and the *User Guide*, is common across multiple products and might describe capabilities that are not available in your deployment. For example, IBM QRadar on Cloud users do not have full administrative capabilities as described in the *IBM QRadar Administration Guide*.

Supported web browsers

For the features in IBM QRadar products to work properly, you must use a supported web browser. The following table lists the supported versions of web browsers.

Table 2. Supported web browsers for QRadar products	
Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported as of QRadar 7.4.0.

Security exceptions and certificates

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla Firefox web browser documentation.

Navigate the web-based application

When you use QRadar, use the navigation options available in the QRadar user interface instead of your web browser **Back** button.

Chapter 3. User management

You define user roles, security profiles, and user accounts to control who has access to IBM QRadar, which tasks they can perform, and which data they have access to.

Use the IBM QRadar on Cloud Self Serve app to define user accounts. To delete user accounts, open a support ticket. For more information, see [QRadar on Cloud work items that require a support ticket](#).

Related concepts

[Capabilities in your IBM QRadar product](#)

Security profiles

Security profiles define which networks, log sources, and domains that a user can access.

QRadar includes one default security profile for administrative users. The **Admin** security profile includes access to all networks, log sources, and domains.

Before you add user accounts, you must create more security profiles to meet the specific access requirements of your users.

Domains

Security profiles must be updated with an associated domain. You must define domains on the **Domain Management** window before the **Domains** tab is shown on the **Security Profile Management** window. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

Domain assignments take precedence over all settings on the **Permission Precedence**, **Networks**, and **Log Sources** tabs.

If the domain is assigned to a tenant, the tenant name appears in brackets beside the domain name in the **Assigned Domains** window.

Permission precedence

Permission precedence determines which security profile components to consider when the system displays events in the **Log Activity** tab and flows in the **Network Activity** tab.

Choose from the following restrictions when you create a security profile:

- **No Restrictions** - This option does not place restrictions on which events are displayed in the **Log Activity** tab, and which flows are displayed in the **Network Activity** tab.
- **Network Only** - This option restricts the user to view only events and flows that are associated with the networks that are specified in this security profile.
- **Log Sources Only** - This option restricts the user to view only events that are associated with the log sources that are specified in this security profile.
- **Networks AND Log Sources** - This option allows the user to view only events and flows that are associated with the log sources and networks that are specified in this security profile.

For example, if the security profile allows access to events from a log source but the destination network is restricted, the event is not displayed in the **Log Activity** tab. The event must match both requirements.

- **Networks OR Log Sources** - This option allows the user to view events and flows that are associated with either the log sources or networks that are specified in this security profile.

For example, if a security profile allows access to events from a log source but the destination network is restricted, the event is displayed on the **Log Activity** tab if the permission precedence is set to **Networks**

OR Log Sources. If the permission precedence is set to **Networks AND Log Sources**, the event is not displayed on the **Log Activity** tab.

Permission precedence for offense data

Security profiles automatically use the **Networks OR Log Sources** permission when offense data is shown. For example, if an offense has a destination IP address that your security profile permits you to see, but the security profile does not grant permissions to the source IP address, the **Offense Summary** window shows both the destination and source IP addresses.

Creating a security profile

To add user accounts, you must first create security profiles to meet the specific access requirements of your users.

About this task

IBM QRadar SIEM includes one default security profile for administrative users. The Admin security profile includes access to all networks, log sources, and domains.

To select multiple items on the **Security Profile Management** window, hold the Control key while you select each network or network group that you want to add.

If after you add networks, log sources or domains you want to remove one or more before you save the configuration, you can select the item and click the **Remove (<)** icon. To remove all items, click **Remove All**.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click the **Security Profiles** icon.
4. On the **Security Profile Management window** toolbar, click **New**.
5. Configure the following parameters:
 - a) In the **Security Profile Name** field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.
 - b) OptionalType a description of the security profile. The maximum number of characters is 255.
6. Click the **Permission Precedence** tab.
7. In the Permission Precedence Setting pane, select a permission precedence option. See [“Permission precedence” on page 11](#).
8. Configure the networks that you want to assign to the security profile:
 - a) Click the **Networks** tab.
 - b) From the navigation tree in the left pane of the **Networks** tab, select the network that you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the network to the Assigned Networks pane.
 - d) Repeat for each network you want to add.
9. Configure the log sources that you want to assign to the security profile:
 - a) Click the **Log Sources** tab.
 - b) From the navigation tree in the left pane, select the log source group or log source you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the log source to the Assigned Log Sources pane.
 - d) Repeat for each log source you want to add.

10. Configure the domains that you want to assign to the security profile:
 - a) Click the **Domains** tab.
 - b) From the navigation tree in the left pane, select the domain that you want this security profile to have access to.
 - c) Click the **Add (>)** icon to add the domain to the Assigned Domains pane.
 - d) Repeat for each domain that you want to add.
11. Click **Save**.

Note: The log sources and domains that are assigned to the security profile must match. You cannot save the security profile if the log sources and domains do not match.
12. Close the **Security Profile Management** window.
13. On the **Admin** tab, click **Deploy Changes**.


Editing a security profile

You can edit an existing security profile to update which networks and log sources a user can access and the permission precedence.

About this task

To quickly locate the security profile you want to edit on the **Security Profile Management** window, type the security profile name in the **Type to filter** text box. It is located above the left pane.

Procedure

1. On the navigation menu () , click **Admin**.
2. Click **System Configuration > User Management**.
3. Click the **Security Profiles** icon.
4. In the left pane, select the security profile you want to edit.
5. On the toolbar, click **Edit**.
6. Update the parameters as required.
7. Click **Save**.
8. If the **Security Profile Has Time Series Data** window opens, select one of the following options:

Option	Description
Keep Old Data and Save	Select this option to keep previously accumulated time series data. If you choose this option, users with this security profile might see previous data that they no longer have permission to see when they view time series charts.
Hide Old Data and Save	Select this option to hide the time series data. If you choose this option, time series data accumulation restarts after you deploy your configuration changes.

9. Close the **Security Profile Management** window.
10. On the **Admin** tab, click **Deploy Changes**.


Duplicating a security profile

If you want to create a new security profile that closely matches an existing security profile, you can duplicate the existing security profile and then modify the parameters.

About this task

To quickly locate the security profile you want to duplicate on the Security Profile Management window, you can type the security profile name in the **Type to filter** text box, which is located above the left pane.

Procedure

1. On the navigation menu (), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Security Profiles**.
4. In the left pane, select the security profile you want to duplicate.
5. On the toolbar, click **Duplicate**.
6. In the **Confirmation** window, type a unique name for the duplicated security profile.
7. Click **OK**.
8. Update the parameters as required.
9. Close the **Security Profile Management** window.
10. On the **Admin** tab, click **Deploy Changes**.

Deleting a security profile


If a security profile is no longer required, you can delete the security profile.

About this task

If user accounts are assigned to the security profiles you want to delete, you must reassign the user accounts to another security profile. IBM QRadar SIEM automatically detects this condition and prompts you to update the user accounts.

To quickly locate the security profile you want to delete on the **Security Profile Management** window, you can type the security profile name in the **Type to filter** text box. It is located above the left pane.

Procedure

1. On the navigation menu (), click **Admin**.
2. Click **System Configuration > User Management**.
3. Click **Security Profiles**.
4. In the left pane, select the security profile that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.
7. Reassign the listed user accounts to another security profile:
 - a) From the **User Security Profile to assign** list box, select a security profile.
 - b) Click **Confirm**.
8. Close the **Security Profile Management** window.
9. On the **Admin** tab, click **Deploy Changes**.

Enterprise Federation authentication

Enterprise Federation is an authentication model that allows an enterprise's IdP (Identity Provider) to authenticate users instead of IBMId authentication. You can use Enterprise Federation to authenticate users to IBM QRadar on Cloud.

For more information, see <https://ibm.ent.box.com/notes/78040808400?v=IBMId-Federation-Guide>.

Chapter 4. System management

IBM QRadar has a modular architecture that supports deployments of varying sizes and topologies.

In a single-host deployment, all the software components run on a single appliance, and the QRadar Console provides the user interface, the real-time event and flow views, reports, offenses, asset information, and administrative functions.

To scale QRadar, you can add non-console managed hosts to the deployment. You can configure a specific component type, such as data gateways, processors, and data nodes, for each managed host, providing greater flexibility to manage data collection and processing in a distributed environment.

Related concepts

[Capabilities in your IBM QRadar product](#)

System health information

The QRadar Deployment Intelligence app is a powerful monitoring application that consolidates historical health data for each managed host in your deployment. Use the app to monitor the health of your QRadar deployment.

The **Host status overview** on the QRadar Deployment Intelligence dashboard shows the state of each appliance (active, standby, offline, or unknown), and the number of notifications for each host, the host name and appliance type, disk usage, status, and time changed. From the **Host status overview**, you can drill down to see more visual information about the status of the managed host, including the event and flow rates, system notifications, and disk information.

To assist with troubleshooting issues in your deployment, use the **Get Logs** capability to collect log files from the QRadar Console and any other managed hosts in your deployment.

The QRadar Deployment Intelligence app is available on the IBM Security App Exchange. You must install the app and then create an authorized service token to allow the app to use the QRadar API to request data from the managed hosts.

The QRadar Deployment Intelligence app uses QRadar health metrics to monitor your deployment. Health metrics are essential, lightweight system events that do not count against your license.

QRadar component types

Each IBM QRadar appliance that is added to the deployment has configurable components that specify the way that the managed host behaves in QRadar.

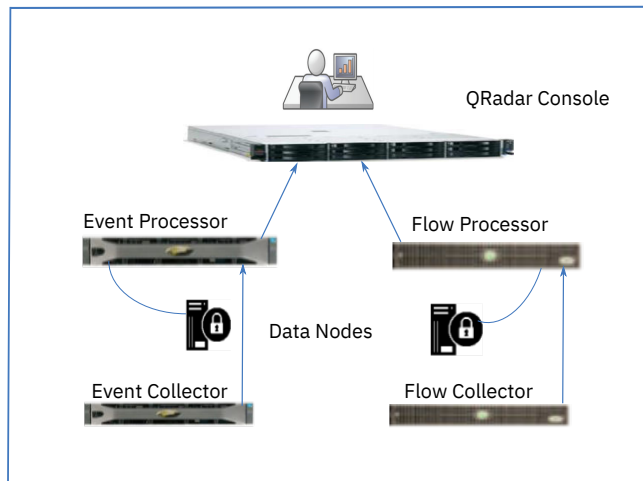


Figure 5. QRadar event and flow components

QRadar Console

The QRadar Console provides the QRadar product interface, real-time event and flow views, reports, offenses, asset information, and administrative functions. In distributed environments, the QRadar Console is used to manage the other components in the deployment.

Event Collector

The Event Collector collects events from local and remote log sources, and normalizes the raw event data so that it can be used by QRadar. To conserve system resources, the Event Collector bundles identical events together and sends the data to the Event Processor.

Event Processor

The Event Processor processes events that are collected from one or more Event Collector components. If events are matched to the custom rules that are defined on the Console, the Event Processor follows the action that is defined in the rule response.

Each Event Processor has local storage. Event data is stored on the processor, or it can be stored on a Data Node.

QRadar QFlow Collector

QRadar QFlow Collector collects network flows from devices on your network. Live and recorded feeds are included, such as network taps, span ports, NetFlow, and QRadar flow logs.

Restriction: QRadar Log Manager doesn't support flow collection.

Flow Processor

The Flow Processor processes flows from one or more QRadar QFlow Collector appliances. The Flow Processor appliance can also collect external network flows such as NetFlow, J-Flow, and sFlow directly from routers in your network.

Flow Processors include an on-board processor and internal storage for flow data.

Data Node

The Data Node receives security events and flows from event and flow processors, and stores the data to disk.

The Data Node is always connected to either an Event Processor or a Flow Processor.

Off-site source and target appliances

An off-site appliance is a QRadar appliance that is not part of the deployment that is monitored by the QRadar Console.

An off-site source appliance forwards normalized data to an Event Collector. You can configure an off-site source to encrypt the data before forwarding.

An off-site target appliance receives normalized event or flow data from any Event Collector, or any processor in your deployment.

Later versions of QRadar systems can receive data from earlier versions of QRadar systems, but earlier versions can't receive data from later versions. To avoid problems, upgrade all receivers before you upgrade senders.

Data nodes

A data node is an appliance that you can add to your event and flow processors to increase storage capacity and improve search performance. You can add an unlimited number of data nodes to your IBM QRadar deployment, and they can be added at any time. Each data node can be connected to only one processor, but a processor can support multiple data nodes.

For more information about planning your deployment, see the *IBM QRadar Architecture and Deployment Guide*.

QRadar system time

When your deployment spans multiple time zones, configure all appliances to use the same time zone as the IBM QRadar Console. Alternatively, you can configure all appliances to use Greenwich Mean Time (GMT).

Configure the IBM QRadar system time from the QRadar user interface. You can configure the time manually, or by configuring Network Time Protocol (NTP) servers to maintain the system time.

You cannot sync external device clocks to IBM QRadar on Cloud. QRadar on Cloud doesn't use a public NTP system to sync. Instead, it syncs by using the IBM Cloud GPS-based time service.

The time is automatically synchronized between the QRadar Console and the managed hosts.

Problems that are caused by mismatched time zones

To ensure that searches and data-related functions work properly, all appliances must synchronize time settings with the QRadar Console appliance. When the time zone settings are mismatched, you might see inconsistent results between QRadar searches and report data.

The Accumulator service runs on all appliances with local storage to create minute by minute accumulations, and hourly and daily roll ups. QRadar uses the accumulated data in reports and time series graphs. When the time zones are mismatched in a distributed deployment, report and time series

graphs might show inconsistent results when compared to AQL query results due to the way that the accumulated data is aggregated.

QRadar searches run against data that is stored in the Ariel databases, which use a date structure (YYYY/MM/DD/HH/MM) to store files to disk. Changing the time zone after the data is written to disk disrupts the file naming sequence in the Ariel databases and might cause data integrity problems.

NAT-enabled networks

Network address translation (NAT) converts an IP address in one network to a different IP address in another network. NAT provides increased security for your IBM QRadar deployment because requests are managed through the conversion process and internal IP addresses are hidden. With NAT, computers that are located on a private, internal network are converted through a network device, typically a firewall, and can communicate to the public internet through that network. Use NAT to map individual internal IP addresses to individual external IP addresses.

QRadar NAT configuration requires static NAT and allows only one public IP address per managed host.

Any QRadar host that is not in the same NAT group with its peer, or is in a different NAT group, is configured to use the public IP address of that host to reach it. For example, when you configure a public IP address on the QRadar Console, any host that is located in the same NAT group uses the private IP address of the QRadar Console to communicate. Any managed host that is located in a different NAT group uses the public IP address of the QRadar Console to communicate.

If you have a host in one of these NAT group locations that does not require external conversion, enter the private IP address in both the **Private IP** and **Public IP** fields. Systems in remote locations with a different NAT group than the console still require an external IP address and NAT, because they need to be able to establish connections to the console. Only hosts that are located in the same NAT group as the console can use the same public and private IP addresses.

Managed hosts

For greater flexibility over data collection and event and flow processing, build a distributed IBM QRadar deployment by adding non-console managed hosts, such as gateways, processors, and data nodes.

For more information about planning and building your QRadar environment, see the *IBM QRadar Architecture and Deployment Guide*.

Software compatibility requirements

Software versions for all IBM QRadar appliances in the deployment must be at the same version and fix pack level. Deployments that use different versions of software are not supported because mixed software environments can cause rules not to fire, offenses not to be created or updated, and errors in search results.

When a managed host uses a software version that is different than the QRadar console, you might be able to view components that were already assigned to the host, but you cannot configure the component or add or assign new components.

Internet Protocol (IP) requirements

Various combinations of IP protocols are supported when adding non-console managed hosts, as described in the following table:

Table 3. Supported combinations of IP protocols when adding non-console managed hosts				
Managed hosts	QRadar Console (IPv6, single)	QRadar Console (IPv6, HA)	QRadar Console (dual-stack, single)	QRadar Console (dual-stack, HA)
IPv4, single	No	No	Yes*	No
IPv4, HA	No	No	No	No

Table 3. Supported combinations of IP protocols when adding non-console managed hosts (continued)				
Managed hosts	QRadar Console (IPv6, single)	QRadar Console (IPv6, HA)	QRadar Console (dual-stack, single)	QRadar Console (dual-stack, HA)
IPv6, single	Yes	Yes	Yes	No
IPv6, HA	Yes	Yes	Yes	No

Restriction: *By default, you cannot add an IPv4-only managed host to a dual-stack single console. You must run a script to enable an IPv4-only managed host. For more information, see [Adding an IPv4-only managed host in a dual-stack environment](#).

A dual-stack console supports both IPv4 and IPv6. The following list outlines the conditions you must follow in dual-stack environments:

- You can add IPv6 managed hosts to a dual-stack single console, or to an IPv6-only console.
- You can add only IPv4 managed hosts to a dual-stack single console.
- Do not add a managed host to a dual-stack console that is configured for HA.
- Do not add an IPv4 managed host that is not in an HA pair to an IPv6-only console, or to a dual-stack console that is in an HA pair.

Important: IBM does not support the following configurations:

- Adding a managed host to a dual-stack console that is configured for HA
- Adding an IPv4 managed host that is not in an HA pair to an IPv6-only console
- Adding an IPv4 managed host that is not in an HA pair to a dual-stack console that is in an HA pair

Bandwidth considerations for managed hosts

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the IBM QRadar console and all managed hosts. Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS).

An Event Collector that is configured to store and forward data to an Event Processor forwards the data according to the schedule that you set. Ensure that you have sufficient bandwidth to cover the amount of data that is collected, otherwise the forwarding appliance cannot maintain the scheduled pace.

Use the following methods to mitigate bandwidth limitations between data centers:

Process and send data to hosts at the primary data center

Design your deployment to process and send data as it's collected to hosts at the primary data center where the console resides. In this design, all user-based searches query the data from the local data center rather than waiting for remote sites to send back data.

You can deploy a store and forward event collector, such as a QRadar 15XX physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

Don't run data-intensive searches over limited bandwidth connections

Ensure that users don't run data-intensive searches over links that have limited bandwidth. Specifying precise filters on the search limits the amount of data that is retrieved from the remote locations, and reduces the bandwidth that is required to send the query result back.

Encryption

To provide secure data transfer between each of the appliances in your environment, IBM QRadar has integrated encryption support that uses OpenSSH. Encryption occurs between managed hosts; therefore, you must have at least one managed host before you can enable encryption.

When encryption is enabled, a secure tunnel is created on the client that initiates the connection, by using an SSH protocol connection. When you enable encryption on a managed host, an SSH tunnel is created for

all client applications on the managed host. When you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console. To ensure that all data between managed hosts is encrypted, enable encryption.

For example, with encryption enabled on an Event Processor, the connection between the Event Processor and Event Collector is encrypted, and the connection between the Event Processor and Magistrate is encrypted.

The SSH tunnel between two managed hosts can be initiated from the remote host instead of the local host. For example, if you have a connection from an Event Processor in a secure environment to an Event Collector that is outside of the secure environment, and you have a firewall rule that would prevent you from having a host outside the secure environment connect to a host in the secure environment, you can switch which host creates the tunnel so that the connection is established from the Event Processor by selecting the **Remote Tunnel Initiation** checkbox for the Event Collector.

You cannot reverse the tunnels from your Console to managed hosts.

Email servers

QRadar uses an email server to distribute alerts, reports, notifications, and event messages.

You can configure an email server for your entire QRadar deployment, or multiple email servers.

If you configure the mail server setting for a host as `localhost`, then the mail messages don't leave that host.

Adding an email server

Add one or more email servers to distribute alerts, reports, notifications, and event messages from your hosts.

Procedure

1. Click the **Admin** tab.
2. Click **Email Server Management**.
3. Click **Add**.
4. Enter the following parameters:

Parameter	Description
Hostname	The hostname of the email server.
Port	The port that mail is sent to on the email server.
Description	A description of the email server, so you can tell it apart from other email servers that you add.
Username	Optional. If you want to send authenticated email, enter the username for SMTP authentication on the target email server.
Password	Optional. If you want to send authenticated email, enter the password for SMTP authentication on the target email server.

5. Optional: Select the **TLS** checkbox to send encrypted email. Sending encrypted email requires an external TLS certificate.
6. Click **Save**.

What to do next

[“Assigning an email server to a host” on page 21](#)

Assigning an email server to a host

After you have configured an email server, assign it to one or more hosts.

Procedure

1. On the **System And License Management** page, select a host.
2. Click **Actions > View and Manage System**.
3. Click the **Email Server** tab.
4. Select an email server and click **Save**.
5. Optional: Test the connection to the email server by clicking the **Test Connection** button.
6. Click **Save**.

Editing an email server

You can edit email server settings if needed.

Procedure

1. Click the **Admin** tab.
2. Click **Email Server Management**.
3. Click the **Other Settings** (⚙️) icon for the server that you are editing.
4. Make whatever changes you need and then click **Save**.

Deleting an email server

Delete an email server if you are no longer using it.

Procedure

1. Click the **Admin** tab.
2. Click **Email Server Management**.
3. Click the **Other Settings** (⚙️) icon for the server that you are deleting.
4. Select **Delete**.

Configuration changes in your QRadar environment

When you make configuration changes to IBM QRadar, the changes are saved to a staging area, and the deployment banner on the **Admin** tab is updated indicating that changes need to be deployed. Deploying the changes might require QRadar services to restart.

QRadar has two methods of deploying changes: standard and full configuration. The type of deployment that is required depends on the type of changes that were made.

Standard deployment

This deployment method restarts only those services that are directly affected by the changes that were made. You begin a standard deployment by clicking **Deploy changes** on the banner on the **Admin** tab.

The following list shows examples of changes that require a standard deployment:

- Adding or editing a new user or user role.
- Setting a password for another user.
- Changing a users' role or security profile.

Full configuration deployment

Changes that affect the entire QRadar deployment must be deployed by using the full configuration deployment method. You begin a full configuration deployment by clicking **Deploy full configuration** from the **Advanced** menu on the **Admin** tab.

This method rebuilds all configuration files on each of the managed hosts. To ensure that the new configuration is loaded properly, all services on the managed hosts are automatically restarted, except for the event collection service. While the other services restart, QRadar continues collecting events and stores them in a buffer until the managed hosts come back online.

The following list shows examples of changes that require a full configuration deployment:

- Adding a managed host.
- Changing the configuration for a managed host.
- Configuring offsite hosts for sending or receiving data from the QRadar Console.
- Restoring a configuration backup.

Changes that impact event collection

Events come into QRadar through the `ecs-ec-ingress` event collection service. Starting in QRadar V7.3.1, the service is managed separately from other QRadar services. To minimize interruptions in collecting event data, the service does not automatically restart when the `hostcontext` service restarts.

The following situations can cause an interruption in event collection:

- Rebooting an appliance that collects events.
- Adding an HA managed host.
- During HA failover.
- Restoring a configuration backup.
- Adding or removing an off-site source connection
- Whenever a partition's disk usage exceeds the maximum threshold.

When you deploy changes after you restore a configuration backup, you can restart the event collection service now or later. When you choose to restart the service later, QRadar deploys all changes that don't depend on the event collection service, and continues to collect events while the other services restart. The deployment banner continues to show undeployed changes, and the `Event collection service must be restarted` message is shown when you view the details.

Configuring an Event Collector

Add a QRadar Event Collector when you want to expand your deployment, either to collect more events locally or collect events from a remote location.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Click **System Configuration > System and License Management**.
3. Select the managed host that you want to configure.
4. Click **Deployment Actions > Edit Host**.
5. Click **Component Management**.
6. Enter values for the following parameters:

Parameter	Description
Event Forwarding Listen Port	The Event Collector event forwarding port.
Flow Forwarding Listen Port	The Event Collector flow forwarding port.

Parameter	Description
Autodetection Enabled	<p>True enables the Event Collector to automatically analyze and accept traffic from previously unknown log sources. The appropriate firewall ports are opened to enable Autodetection to receive events. This option is the default.</p> <p>False prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources.</p> <p>For more information, see the <i>Managing Log Sources Guide</i>.</p>
Autodetection - Use Global settings	<p>True specifies that the Event Collector uses global settings for Log Source Autodetection.</p> <p>False specifies that the Event Collector uses individual, local settings (XML configuration file) for Log Source Autodetection.</p>
Flow Deduplication Enabled	
Flow Deduplication Filter Time	The amount of time in seconds that flows are buffered before they are forwarded.
Asymmetric Flow Filter Time	The amount of time in seconds that asymmetric flow is buffered before they are forwarded.
Forward Events Already Seen	<p>True enables the Event Collector to forward events that were detected on the system.</p> <p>False prevents the Event Collector from forwarding events that were detected on the system. This option prevents event-looping on your system.</p>
Compress Event Processor Traffic	

7. Click **Save**.

8. Repeat for all QRadar Event Collectors in your deployment that you want to configure.

Deploying changes

Changes that are made to the IBM QRadar deployment must be pushed from the staging area to the production area.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. Check the deployment banner to determine whether changes must be deployed.
3. Click **View Details** to view information about the undeployed configuration changes.
4. Choose the deployment method:
 - a) To deploy changes and restart only the affected services, click **Deploy Changes** on the deployment banner.
 - b) To rebuild the configuration files and restart all services on each managed host, click **Advanced > Deploy Full Configuration**.

Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

Restarting the event collection service

There might be situations when you want to restart only the event collection service across all managed hosts in your IBM QRadar environment. For example, when a new version of the **ecs-ec-ingress** service is available for upgrade, or when you deferred restarting the service during an earlier deployment.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. On the **Advanced** menu, click **Restart Event Collection Services**. Event collection is briefly interrupted while the service restarts.

Resetting SIM

After you tune your deployment, avoid receiving any additional false positive information by resetting SIM to remove all offense, and source and destination IP addresses from the database and the disk.

About this task

The SIM reset process can take several minutes, depending on the amount of data in your system. If you attempt to move to other areas of the IBM QRadar user interface during the SIM reset process, an error message is displayed.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. From the **Advanced** menu, select **Clean SIM Model**.
3. Read the information on the **Reset SIM Data Model** window.
4. Select one of the following options.

Option	Description
Soft Clean	Closes all offenses in the database. If you select the Soft Clean option, you can also select the Deactivate all offenses check box.
Hard Clean	Purges all current and historical SIM data from the database, including protected offenses, source IP addresses, and destination IP addresses.

5. If you want to continue, select the **Are you sure you want to reset the data model?** check box.
6. Click **Proceed**.
7. When the SIM reset process is complete, click **Close**.
8. Refresh your web browser.

Chapter 5. QRadar setup tasks

Use the settings on the Admin tab to configure your IBM QRadar deployment, including your network hierarchy, automatic updates, system settings, event retention buckets, system notifications, console settings, and index management.

Related concepts

[Capabilities in your IBM QRadar product](#)

Network hierarchy

IBM QRadar uses the network hierarchy objects and groups to view network activity and monitor groups or services in your network.

When you develop your network hierarchy, consider the most effective method for viewing network activity. The network hierarchy does not need to resemble the physical deployment of your network. QRadar supports any network hierarchy that can be defined by a range of IP addresses. You can base your network on many different variables, including geographical or business units.

Related concepts

[Network hierarchy updates in a multitenant deployment](#)

Guidelines for defining your network hierarchy

Building a network hierarchy in IBM QRadar is an essential first step in configuring your deployment. Without a well configured network hierarchy, QRadar cannot determine flow directions, build a reliable asset database, or benefit from useful building blocks in rules.

Consider the following guidelines when you define your network hierarchy:

- Organize your systems and networks by role or similar traffic patterns.

For example, you might organize your network to include groups for mail servers, departmental users, labs, or development teams. Using this organization, you can differentiate network behavior and enforce behaviour-based network management security policies. However, do not group a server that has unique behavior with other servers on your network. Placing a unique server alone provides the server greater visibility in QRadar, and makes it easier to create specific security policies for the server.

- Place servers with high volumes of traffic, such as mail servers, at the top of the group. This hierarchy provides you with a visual representation when a discrepancy occurs.
- Do not configure a network group with more than 15 objects.

Large network groups can cause difficulty when you view detailed information for each object. If your deployment processes more than 600,000 flows, consider creating multiple top-level groups.

- Conserve disk space by combining multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network group.

For example, add key servers as individual objects, and group other major but related servers into multi-CIDR objects.

Table 4. Example of multiple CIDRs and subnets in a single network group		
Group	Description	IP addresses
1	Marketing	10.10.5.0/24
2	Sales	10.10.8.0/21

Table 4. Example of multiple CIDRs and subnets in a single network group (continued)		
Group	Description	IP addresses
3	Database Cluster	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

- Define an all-encompassing group so that when you define new networks, the appropriate policies and behavior monitors are applied.

In the following example, if you add an HR department network, such as 10.10.50.0/24, to the Cleveland group, the traffic displays as Cleveland-based and any rules you apply to the Cleveland group are applied by default.

Table 5. Example of an all-encompassing group		
Group	Subgroup	IP address
Cleveland	Cleveland miscellaneous	10.10.0.0/16
Cleveland	Cleveland Sales	10.10.8.0/21
Cleveland	Cleveland Marketing	10.10.1.0/24

- In a domain-enabled environment, ensure that each IP address is assigned to the appropriate domain.

Related information

[QRadar Support Geodata FAQ](#)

Acceptable CIDR values

IBM QRadar accepts specific CIDR values.

The following table provides a list of the CIDR values that QRadar accepts:

Table 6. Acceptable CIDR values			
CIDR Length	Mask	Number of Networks	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136

Table 6. Acceptable CIDR values (continued)			
CIDR Length	Mask	Number of Networks	Hosts
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 subnets	124
/26	255.255.255.192	4 subnets	62
/27	255.255.255.224	8 subnets	30
/28	255.255.255.240	16 subnets	14
/29	255.255.255.248	32 subnets	6
/30	255.255.255.252	64 subnets	2
/31	255.255.255.254	none	none
/32	255.255.255.255	1/256 C	1

For example, a network is called a supernet when the prefix boundary contains fewer bits than the natural (or classful) mask of the network. A network is called a subnet when the prefix boundary contains more bits than the natural mask of the network:

- 209.60.128.0 is a class C network address with a mask of /24.
- 209.60.128.0 /22 is a supernet that yields:
 - 209.60.128.0 /24
 - 209.60.129.0 /24
 - 209.60.130.0 /24
 - 209.60.131.0 /24
- 192.0.0.0 /25
 - Subnet Host Range
 - 0 192.0.0.1-192.0.0.126
 - 1 192.0.0.129-192.0.0.254
- 192.0.0.0 /26
 - Subnet Host Range
 - 0 192.0.0.1 - 192.0.0.62
 - 1 192.0.0.65 - 192.0.0.126
 - 2 192.0.0.129 - 192.0.0.190

- 3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27
- Subnet Host Range
- 0 192.0.0.1 - 192.0.0.30
- 1 192.0.0.33 - 192.0.0.62
- 2 192.0.0.65 - 192.0.0.94
- 3 192.0.0.97 - 192.0.0.126
- 4 192.0.0.129 - 192.0.0.158
- 5 192.0.0.161 - 192.0.0.190
- 6 192.0.0.193 - 192.0.0.222
- 7 192.0.0.225 - 192.0.0.254

Related tasks

[Defining your network hierarchy](#)

A default network hierarchy that contains pre-defined network groups is included in IBM QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Defining your network hierarchy


A default network hierarchy that contains pre-defined network groups is included in IBM QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

About this task

Network objects are containers for Classless Inter-Domain Routing (CIDR) addresses. Any IP address that is defined in a CIDR range in the network hierarchy is considered to be a local address. Any IP address that is not defined in a CIDR range in the network hierarchy is considered to be a remote address. A CIDR can belong only to one network object, but subsets of a CIDR range can belong to another network object. Network traffic matches the most exact CIDR. A network object can have multiple CIDR ranges assigned to it.

Some of the default building blocks and rules in QRadar use the default network hierarchy objects. Before you change a default network hierarchy object, search the rules and building blocks to understand how the object is used and which rules and building blocks might need adjustments after you modify the object. It is important to keep the network hierarchy, rules, and building blocks up-to-date to prevent false offenses.

Procedure

1. On the navigation menu (), click **Admin**.
2. In the **System Configuration** section, click **Network Hierarchy**.
3. From the menu tree on the **Network Views** window, select the area of the network in which you want to work.
4. To add network objects, click **Add** and complete the following fields:

Option	Description
Name	<p>The unique name of the network object.</p> <p>Tip: You can use periods in network object names to define network object hierarchies. For example, if you enter the object name D . E . F, you create a three-tier hierarchy with E as a subnode of D, and F as a subnode of E.</p>

Option	Description
Group	The network group in which to add the network object. Select from the Group list, or click Add a New Group . Tip: When you add a network group, you can use periods in network group names to define network group hierarchies. For example, if you enter the group name A . B . C, you create a three-tier hierarchy with B as a subnode of A, and C as a subnode of B.
IP/CIDR(s)	Type an IP address or CIDR range for the network object, and click Add . You can add multiple IP addresses and CIDR ranges.
Description	A description of the network object. This field is optional.
Country/Region	The country or region in which the network object is located. This field is optional.
Longitude and Latitude	The geographic location (longitude and latitude) of the network object. These fields are co-dependent and optional.

- Click **Create**.
- Repeat the steps to add more network objects, or click **Edit** or **Delete** to work with existing network objects.

Related concepts

[Acceptable CIDR values](#)

IBM QRadar accepts specific CIDR values.

IF-MAP server certificates

The Interface For Metadata Access Points (IF-MAP) rule response enables the IBM QRadar console to publish alert and offense data that is derived from events, flows, and offenses to an IF-MAP server.

Configuring IF-MAP Server Certificate for Basic Authentication

This task provides instruction for how to configure your IF-MAP certificate for basic authentication.

Before you begin

Contact your IF-MAP server administrator to obtain a copy of the IF-MAP server public certificate. The certificate must have the .cert file extension.

Procedure

- Using SSH, log in to IBM QRadar as the root user.
- Copy the certificate to the /opt/qradar/conf/trusted_certificates directory.

SSL certificates

Secure Sockets Layer (SSL) is an industry standard security protocol is used by websites to protect online transactions. It provides communication privacy so that client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. To generate an SSL link, a web server requires an SSL certificate. SSL certificates are issued by internal or trusted third-party certifying authorities.

Browsers and operating systems include a preinstalled list of trusted certificates, which are installed in the Trusted Root Certification authorities store.

Self-signed certificates

A self-signed certificate provides basic security, enabling data encryption between the user and the application. Because self-signed certificates cannot be authenticated by any existing known root certificate authorities, users are warned about this unknown certificate and must accept it to proceed.

Internal CA signed certificates

Organizations that have their own internal root certificate authority (CA) can create a certificate by using that internal CA. This certificate is supported by QRadar, and the internal root CA is also imported into the QRadar environment.

Public CA / Intermediate CA signed

Certificates that are signed by known public CAs and intermediate certificates are supported by QRadar.

Public signed certificates can be used directly in QRadar, and certificates that are signed with Intermediate CA are installed by using both the signed certificate and the intermediate certificate to provide valid certificate functions.

Note: An intermediate certificate is commonly used by organizations that create multiple SSL keys in their environment, and want to have them signed by a known commercial certificate vendor. When they use the intermediate key, they can then create sub-keys from this intermediate key. When this configuration is used, QRadar must be configured with both the intermediate certificate and the host SSL certificate so that connections to the host can verify the full certificate path.

Related information

How to view SSL certificate details (<https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details>)

SSL connections between QRadar components

To establish all internal SSL connections between components, QRadar uses the web server certificate that is preinstalled on the QRadar Console.

All trusted certificates for QRadar must meet the following requirements:

- The certificate must be an X.509 certificate and have PEM base64 encoding.
- The certificate must have a .cert, .crt, .pem, or .der file extension.
- Keystore files that contain certificates must have the .truststore file extension.
- The certificate file must be stored in the /opt/qradar/conf/trusted_certificates directory.

IPv6 addressing in QRadar deployments

IPv4 and IPv6 addressing is supported for network connectivity and management of IBM QRadar software and appliances. When you install QRadar, you are prompted to specify whether your Internet Protocol is IPv4 or IPv6.

QRadar components that support IPv6 addressing

The following QRadar components support IPv6 addressing.

Network Activity tab

Because **IPv6 Source Address** and **IPv6 Destination Address** are not default columns, they are not automatically displayed. To display these columns, you must select them when you configure your search parameters (column definition).

To save space and indexing in an IPv4 or IPv6 source environment, extra IP address fields are not stored or displayed. In a mixed IPv4 and IPv6 environment, a flow record contains both IPv4 and IPv6 addresses.

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow might not support IPv6.

Log Activity tab

Because **IPv6 Source Address** and **IPv6 Destination Address** are not default columns, they are not automatically displayed. To display these columns, you must select them when you configure your search parameters (column definition).

DSMs can parse IPv6 addresses from the event payload. If any DSM cannot parse IPv6 addresses, a log source extension can parse the addresses. For more information about log source extensions, see the *DSM Configuration Guide*.

Searching, grouping, and reporting on IPv6 fields

You can search events and flows by using IPv6 parameters in the search criteria.

You can also group and sort event and flow records that are based on IPv6 parameters.

You can create reports that are based on data from IPv6-based searches.

Custom rules

In custom rules and building blocks, IP parameters support IPv4 and IPv6 addresses unless the parameters are labeled as one or the other (for example, **SRC IPv6** supports only IPv6 addresses).

Device support modules (DSMs)

DSMs can parse IPv6 source and destination address from event payloads.

Deploying QRadar in IPv6 or mixed environments

To log in to QRadar in an IPv6 or mixed environment, wrap the IP address in square brackets. For example, `https://[<IP Address>]`

Both IPv4 and IPv6 environments can use a hosts file for address translation. In an IPv6 or mixed environment, the client resolves the Console address by its host name. You must add the IP address of the IPv6 console to the `/etc/hosts` file on the client.

Flow sources, such as NetFlow and sFlow, are accepted from IPv4 and IPv6 addresses. Event sources, such as syslog and SNMP, are accepted from IPv4 and IPv6 addresses. You can disable superflows and flow bundling in an IPv6 environment.

Restriction: By default, you cannot add an IPv4-only managed host to an IPv6 and IPv4 mixed-mode console. You must run a script to enable an IPv4-only managed host.

IPv6 addressing limitations

When QRadar is deployed in an IPv6 environment, the following limitations are known:

- Some parts of the QRadar deployment do not take advantage of the IPv6-enabled network hierarchy, including surveillance, searching, and analysis.
- No host profile test in custom rules for IPv6 addresses.
- No specialized indexing or optimization of IPv6 addresses.

Advanced iptables rules examples

You can configure your iptables rules to better control access to QRadar, restrict inbound data sources, and redirect traffic. The following examples can help you to gain better insight to your network, by manually adjusting your iptables.

Blocking iptables access to SSH

Consoles and unmanaged hosts allow SSH from any inbound request. When a host is added to the deployment, the consoles allow SSH access from the QRadar Console, and the console keeps port 22 open for inbound connections. You can limit the inbound connections on port 22 by modifying a host's iptables rules.

You can block SSH access from other managed hosts on your console, which can break encrypted connections.

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.41 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.59 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -j DROP
```

Enabling ICMP to QRadar systems

You can enable ping responses from your QRadar system by adding the following rule to the `/opt/qradar/conf/iptables.pre` file.

```
-A INPUT -p icmp -j ACCEPT
```

Run the following script to create an entry in the `/etc/sysconfig/iptables` file.

Important: You can limit this rule to a specific host by adding the `-s source.ip.address` field.

Blocking unwanted data sources

You can block out a data source such as a log source or a netflow data source, for a short time, rather than disabling the original device. To block a particular host, you can add an entry similar to the following to `/opt/qradar/conf/iptables.pre`.

Block a netflow from the router:

```
-A INPUT -p udp -s <IP Address> --dport 2055 -j REJECT
```

Block a syslog from another source:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Block a syslog from a specific subnet:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Configuring iptables rules

Access to the QRadar network services is controlled first on hosts with iptables. The iptables rules are adjusted and configured based on the requirements of the deployment. Ports for Ariel searching, streaming, and times when you are using encryption (tunneling) can update various iptables rules.

About this task

You can configure and check iptables rules for IPv4 and IPv6. The following procedure indicates how you can tune your iptables manually.

Procedure

1. Log in to QRadar as the root user by using SSH.
Login: `<root>`
Password: `<password>`
2. Type the following command to edit the pre rules iptables file:
IPv4:
`vi /opt/qradar/conf/iptables.pre`
IPv6:

- ```
vi /opt/qradar/conf/ip6tables.pre
```
- The iptables.pre configuration file is displayed.
3. Type the following command to edit the post rules iptables file:  
IPv4:  

```
vi /opt/qradar/conf/iptables.post
```

  
IPv6:  

```
vi /opt/qradar/conf/ip6tables.post
```

  
The iptables.post configuration file is displayed.
  4. Add the following rule for QRadar to access a specific port number, where *portnumber* is the port number:  
  
To accept UDP traffic for a specific port input:  

```
-A INPUT -m udp -p udp --dport <portnumber> -j ACCEPT
```

  
To accept TCP traffic for a specific port input:  

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport <portnumber> -j ACCEPT
```
  5. Save your iptables configuration.
  6. Run the following script to propagate the changes:  

```
/opt/qradar/bin/iptables_update.pl
```
  7. Type the following commands to check for existing iptables:  
IPv4:  

```
iptables -L -n -v
```

  
IPv6:  

```
ip6tables -L -n -v
```

## Data retention

---

Retention buckets define how long event and flow data is retained in IBM QRadar.

As QRadar receives events and flows, each one is compared against the retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the deletion policy time period is reached. The default retention period is 30 days; then, the data is immediately deleted.

Retention buckets are sequenced in priority order from the top row to the bottom row. A record is stored in the bucket that matches the filter criteria with highest priority. If the record does not match any of your configured retention buckets, the record is stored in the default retention bucket, which is always located below the list of configurable retention buckets.

### Tenant data

You can configure up to 10 retention buckets for shared data, and up to 10 retention buckets for each tenant.

When data comes into the system, the data is assessed to determine whether it is shared data or whether the data belongs to a tenant. Tenant-specific data is compared to the retention bucket filters that are defined for that tenant. When the data matches a retention bucket filter, the data is stored in that retention bucket until the retention policy time period is reached.

If you don't configure retention buckets for the tenant, the data is automatically placed in the default retention bucket for the tenant. The default retention period is 30 days, unless you configure a tenant-specific retention bucket.

## Configuring retention buckets

Configure retention policies to define how long IBM QRadar is required to keep event and flow data, and what to do when that data reaches a certain age.

### About this task

Changes to the retention bucket filters are applied immediately to incoming data only. For example, if you configured a retention bucket to retain all data from source IP address 10.0.0.0/8 for 1 day, and you later edit the filter to retain data from source IP 192.168.0.1, the change is not retroactive. Immediately upon changing the filter, the retention bucket has 24 hours of 10.0.0.0/8 data, and all data that is collected after the filter change is 192.168.0.1 data.

The retention policy on the bucket is applied to all data in the bucket, regardless of the filters criteria. Using the previous example, if you changed the retention policy from 1 day to 7 days, both the 10.0.0.0/8 data and the 192.168.0.1 data in the bucket is retained for 7 days.

The **Distribution** of a retention bucket indicates the retention bucket usage as a percentage of total data retention in all your retention buckets. The distribution is calculated on a per-tenant basis.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant that you want the retention bucket to apply to.

**Note:** To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.

4. To configure a new retention bucket, follow these steps:
  - a) Double-click the first empty row in the table to open the **Retention Properties** window.
  - b) Configure the retention bucket parameters.

#### Learn more about retention bucket parameters:

| Properties                                 | Description                                                                                                                                                                                                                                       |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                                | Type a unique name for the retention bucket.                                                                                                                                                                                                      |
| <b>Keep data placed in this bucket for</b> | The retention period that specifies how long the data is to be kept. When the retention period is reached, data is deleted according to the <b>Delete data in this bucket</b> parameter. QRadar does not delete data within the retention period. |

| Properties                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Delete data in this bucket</b> | <p>Select <b>Immediately after the retention period has expired</b> to delete data immediately on matching the <b>Keep data placed in this bucket for</b> parameter. The data is deleted at the next scheduled disk maintenance process, regardless of disk storage requirements.</p> <p>Select <b>When storage space is required</b> to keep data that matches the <b>Keep data placed in this bucket for</b> parameter in storage until the disk monitoring system detects that storage is required.</p> <p>Deletions that are based on storage space begin when the free disk space drops to 15% or less, and the deletions continue until the free disk space is 18% or the policy time frame that is set in the <b>Keep data placed in this bucket for</b> field runs out. For example, if the used disk space reaches 85% for records, data is deleted until the used percentage drops to 82%. When storage is required, only data that matches the <b>Keep data placed in this bucket for</b> field is deleted.</p> <p>If the bucket is set to <b>Delete data in this bucket: immediately after the retention period has expired</b>, no disk space checks are done and the deletion task immediately removes any data that is past the retention.</p> |
| <b>Description</b>                | Type a description for the retention bucket.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Current Filters</b>            | Configure the filter criteria that each piece of data is to be compared against.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

- c) Click **Add Filter** after you specify each set of filter criteria.
- d) Click **Save**.
- 5. To edit an existing retention bucket, select the row from the table and click **Edit**.
- 6. To delete a retention bucket, select the row from the table and click **Delete**.
- 7. Click **Save**.

Incoming data that matches the retention policy properties is immediately stored in the retention bucket.

## Managing retention bucket sequence


You can change the order of the retention buckets to ensure that data is being matched against the retention buckets in the order that matches your requirements.

### About this task

Retention buckets are sequenced in priority order from the top row to the bottom row on the **Event Retention** and **Flow Retention** windows. A record is stored in the first retention bucket that matches the record parameters.

You cannot move the default retention bucket. It always resides at the bottom of the list.

### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant for the retention buckets that you want to reorder.

**Note:** To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.

4. Select the row that corresponds to the retention bucket that you want to move, and click **Up** or **Down** to move it to the correct location.
5. Click **Save**.


## Enabling and disabling a retention bucket

When you configure and save a retention bucket, it is enabled by default. You can disable a bucket to tune your event or flow retention.

### About this task

When you disable a bucket, any new events or flows that match the requirements for the disabled bucket are stored in the next bucket that matches the event or flow properties.


### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant for the retention bucket that you want to change.  
**Note:** To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.
4. Select the retention bucket you want to disable, and then click **Enable/Disable**.

## Deleting a Retention Bucket

When you delete a retention bucket, only the criteria that defines the bucket is deleted. The events or flows that were stored in the bucket are collected by the default retention bucket. The default retention period is 30 days; then, the data is immediately deleted.

### Procedure



1. On the navigation menu () , click **Admin**.
2. In the **Data sources** section, click **Event Retention** or **Flow Retention**.
3. If you configured tenants, in the **Tenant** list, select the tenant for the retention bucket that you want to delete.  
**Note:** To manage retention policies for shared data in a multi-tenant configuration, choose **N/A** in the **Tenant** list.
4. Select the retention bucket that you want to delete, and then click **Delete**.

## System notifications

---

IBM QRadar continuously monitors all appliances and delivers information, warning, and error notifications to the QRadar Console, making it easier for you to monitor the status and health of your deployment.

Global System Notifications are host specific and the threshold for each notification is set automatically by QRadar.

To show system notifications on your screen, you must configure your browser to allow pop-up windows and ensure that the **Enable Popup Notifications** check box is selected in your user preferences (). If you disable desktop notifications for QRadar, you can still view the system notifications under the notifications () menu.

During installation, QRadar automatically determines and configures the thresholds for all system notifications.

For information about system notifications, see the *IBM QRadar Troubleshooting and System Notifications Guide*.

**Note:** Browser notifications are supported for Mozilla Firefox, Google Chrome, and Microsoft Edge 10. Microsoft Internet Explorer does not support browser-based notifications. Notifications in Internet Explorer appear in a QRadar notification box. The way that the notifications appear and how long the messages stay on the screen might vary between browsers.

## Configuring event and flow custom email notifications

When you configure rules in IBM QRadar, specify that each time the rule generates a response, an email notification is sent to recipients. The email notification provides useful information, such as event or flow properties.

### About this task

You can customize the content that is included in the email notification for rule response by editing the `alert-config.xml` file.

**Note:** References to flows do not apply to IBM QRadar Log Manager.

You must create a temporary directory where you can safely edit your copy of the files, without the risk of overwriting the default files. After you edit and save the `alert-config.xml` file, you must run a script that validates your changes. The validation script automatically applies your changes to a staging area. You must deploy the full configuration to rebuild the configuration files for all appliances.

**Important:** For IBM QRadar on Cloud, you must open a ticket with IBM Support to get a copy of the `alert-config.xml` file. You must open another ticket to apply the updated `alert-config.xml` file to your QRadar on Cloud instance.

### Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Create a new temporary directory to use to safely edit copies of the default files.
3. To copy the files that are stored in the `custom_alerts` directory to the temporary directory, type the following command:

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*.xml <directory_name>
```

The `<directory_name>` is the name of the temporary directory that you created.

4. Confirm that the files were copied successfully:
  - a) To list the files in the directory, type `ls -lah`.
  - b) Verify that the `alert-config.xml` file is listed.
5. Open the `alert-config.xml` file for editing.
6. Edit the contents of the `<template>` element.
  - a) Required: Specify the type of template to use. Valid options are `event` or `flow`.

```
<templatetype>event</templatetype>
```

```
<templatetype>flow</templatetype>
```

- b) Type a name for the email template:

```
<templatename>Default flow template</templatename>
```

If you have more than one template, ensure that the template name is unique.

c) Set the <active> element to true:

```
<active>true</active>
```

d) Edit the parameters in the <body> or <subject> elements to include the information that you want to see.

**Important:** The <active></active> property must be set to True for each event and flow template type that you want to appear as an option in QRadar. There must be at least one active template for each type.

You must also ensure that the <filename></filename> property is left empty.

**Notification parameters that you can use in the template:**

| Table 7. Accepted Notification Parameters |                     |                       |
|-------------------------------------------|---------------------|-----------------------|
| Common Parameters                         | Event Parameters    | Flow Parameters       |
| AppName                                   | EventCollectorID    | Type                  |
| RuleName                                  | DeviceId            | CompoundAppID         |
| RuleDescription                           | DeviceName          | FlowSourceIDs         |
| EventName                                 | DeviceTime          | SourceASNList         |
| EventDescription                          | DstPostNATPort      | DestinationASNList    |
| EventProcessorId                          | SrcPostNATPort      | InputIFIndexList      |
| Qid                                       | DstMACAddress       | OutputIFIndexList     |
| Category                                  | DstPostNATIPAddress | AppId                 |
| RemoteDestinationIP                       | DstPreNATIPAddress  | Host                  |
| Payload                                   | SrcMACAddress       | Port                  |
| Credibility                               | SrcPostNATIPAddress | SourceBytes           |
| Relevance                                 | SrcPreNATIPAddress  | SourcePackets         |
| Source                                    | SrcPreNATPor        | Direction             |
| SourcePort                                | DstPreNATPort       | SourceTOS             |
| SourceIP                                  |                     | SourceDSCP            |
| Destination                               |                     | SourcePrecedence      |
| DestinationPort                           |                     | DestinationTOS        |
| DestinationIP                             |                     | DestinationDSCP       |
| DestinationUserName                       |                     | SourceASN             |
| Protocol                                  |                     | DestinationASN        |
| StartTime                                 |                     | InputIFIndex          |
| Duration                                  |                     | OutputIFIndex         |
| StopTime                                  |                     | FirstPacketTime       |
| EventCount                                |                     | LastPacketTime        |
| SourceV6                                  |                     | TotalSourceBytes      |
| DestinationV6                             |                     | TotalDestinationBytes |
| UserName                                  |                     | TotalSourcePackets    |



Table 7. Accepted Notification Parameters (continued)

| Common Parameters        | Event Parameters | Flow Parameters         |
|--------------------------|------------------|-------------------------|
| DestinationNetwork       |                  | TotalDestinationPackets |
| SourceNetwork            |                  | SourceQOS               |
| Severity                 |                  | DestinationQOS          |
| CustomProperty           |                  | SourcePayload           |
| CustomPropertiesList     |                  |                         |
| CalculatedProperty       |                  |                         |
| CalculatedPropertiesList |                  |                         |
| AQLCustomProperty        |                  |                         |
| AqlCustomPropertiesList  |                  |                         |
| LogSourceId              |                  |                         |
| LogSourceName            |                  |                         |

**Note:** If you do not want to retrieve the entire list when you use the CustomProperties, CalculatedProperties, or AqlCustomProperties parameter, you can select a specific property by using the following tags:

- Custom Property: `${body.CustomProperty("<custom_property_name>")}`
- Calculated Property: `${body.CalculatedProperty("<calculated_property_name>")}`
- AQL Custom Property: `${body.AqlCustomProperty("<AQL_custom_property_name>")}`

7. To create multiple email templates, copy and paste the following sample email template in the `<template>` element in the `alert-config.xml` file. Repeat Step 6 for each template that you add.

**Sample email template:**

```
<template>
 <templatename>Default Flow</templatename>
 <templatetype>flow</templatetype>
 <active>true</active>
 <filename></filename>
 <subject>${RuleName} Fired </subject>
 <body>
 The ${AppName} event custom rule engine sent an automated response:

 ${StartTime}

 Rule Name: ${RuleName}
 Rule Description: ${RuleDescription}

 Source IP: ${SourceIP}
 Source Port: ${SourcePort}
 Source Username (from event): ${UserName}
 Source Network: ${SourceNetwork}

 Destination IP: ${DestinationIP}
 Destination Port: ${DestinationPort}
 Destination Username (from Asset Identity): ${DestinationUserName}
 Destination Network: ${DestinationNetwork}

 Protocol: ${Protocol}
 QID: ${Qid}

 Event Name: ${EventName}
 Event Description: ${EventDescription}
 Category: ${Category}

 Log Source ID: ${LogSourceId}
 Log Source Name: ${LogSourceName}
```

```

Payload: ${Payload}
CustomPropertiesList: ${CustomPropertiesList}
AQL Custom Property, CEP_aql_1: ${body.AqlCustomProperty("CEP_aql_1")}
Calculated Property, CEP_calc_2: ${body.CalculatedProperty("CEP_calc_2")}
Regex Property, CEP_reg_3: ${body.CustomProperty("CEP_reg_3")}

</body>
<from></from>
<to></to>
<cc></cc>
<bcc></bcc>
</template>

```


**Note:** Currently, the **DomainID** for multi-tenancy or overlapping IP addresses isn't available in the custom email templates.

8. Save and close the `alert-config.xml` file.
9. Validate the changes by typing the following command.

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

The `<directory_name>` parameter is the name of the temporary directory that you created.

If the script validates the changes successfully, the following message is displayed: File `alert-config.xml` was deployed successfully to staging!

10. Deploy the changes in QRadar.
  - a) Log in to QRadar.
  - b) On the navigation menu () , click **Admin**.
  - c) Click **Advanced** > **Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

## Configuring custom offense email notifications

You can create templates for email notifications that are triggered for offenses.

You customize the content that is included in the email notification by editing the `alert-config.xml` file.

You must create a temporary directory where you can safely edit your copy of the files, without the risk of overwriting the default files. After you edit and save the `alert-config.xml` file, you must run a script that validates your changes. The validation script automatically applies your changes to a staging area. You must deploy the full configuration to rebuild the configuration files for all appliances.

### Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Create a new temporary directory to use to safely edit copies of the default files.
3. Type the following command to copy the files that are stored in the `custom_alerts` directory to the temporary directory:

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*.* <directory_name>
```

The `<directory_name>` is the name of the temporary directory that you created.

If the file does not exist in the staging directory, you might find it in the `/opt/qradar/conf/templates/custom_alerts` directory.

4. Confirm that the files were copied successfully:
  - a) To list the files in the directory, type `ls -lah`.
  - b) Verify that the `alert-config.xml` file is listed.
5. Open the `alert-config.xml` file for editing.
6. Add a new `<template>` element for the new offense template.
  - a) Required: Enter offense for the template type value.

```
<templatetype>offense</templatetype>
```

- b) Type a name for the offense template.  
For example, `<templatename>Default offense template</templatename>`  
If you have more than one template, ensure that the template name is unique.
- c) Set the `<active>` element to true.

```
<active>true</active>
```

**Important:** The `<active></active>` property must be set to `true` for each template type that you want to appear as an option in QRadar. There must be at least one active template for each type.

- d) Edit the parameters in the `<body>` or `<subject>` elements to include the information that you want to see.

The following lists provide the values that you can use in the offense template. \$Label values provide the label for the item and the \$Value values provide the data.

#### Offense parameters

\$Value.DefaultSubject  
\$Value.Intro  
\$Value.OffenseId  
\$Value.OffenseStartTime  
\$Value.OffenseUrl  
\$Value.OffenseMRSC  
\$Value.OffenseDescription  
\$Value.EventCounts  
  
\$Label.OffenseSourceSummary  
\$Value.OffenseSourceSummary  
  
\$Label.TopSourceIPs  
\$Value.TopSourceIPs  
  
\$Label.TopDestinationIPs  
\$Value.TopDestinationIPs  
  
\$Label.TopLogSources  
\$Value.TopLogSources  
  
\$Label.TopUsers  
\$Value.TopUsers

\$Label.TopCategories

\$Value.TopCategories

\$Label.TopAnnotations

\$Value.TopAnnotations

\$Label.ContributingCreRules

\$Value.ContributingCreRules

You can also loop over some values by using the following syntax in the template:

```
#foreach($item in $Value.X)
 $item
#end
```

Where X is one of the following values:

- OffenseSourceSummaryList
- TopSourceIPsList
- TopDestinationIPsList
- TopLogSourcesList
- TopUsersList
- TopCategoriesList
- TopAnnotationsList
- ContributingCreRulesList

You can include the following properties by using `${X}`, where X is one of the following values:

- OffenseID
- OffenseRuleID
- OffenseRuleName
- Magnitude
- Relevance
- Severity
- Credibility
- Domain ("N/A" if not found)
- Tenant ("N/A" if not found)
- OffenseType

For example, if an offense has a magnitude of 7, and you include `${Magnitude}` in the template, the value for `${Magnitude}` appears as 7 in the email.

7. Save and close the alert-config.xml file.


8. Validate the changes by typing the following command.

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

`<directory_name>` is the name of the temporary directory that you created.

If the script validates the changes successfully, the following message is displayed: File alert-config.xml was deployed successfully to staging!

9. Deploy the changes in QRadar.

- a) Log in to QRadar.
- b) On the navigation menu () , click **Admin**.
- c) Click **Advanced > Deploy Full Configuration**.

**Note:** QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

## Custom offense close reasons

---

You can manage the options listed in the **Reason for Closing** list box on the **Offenses** tab.

When a user closes an offense on the **Offenses** tab, the Close Offense window is displayed. The user is prompted to select a reason from the **Reason for Closing** list box. Three default options are listed:


- False-positive, tuned
- Non-issue
- Policy violation

Administrators can add, edit, and delete custom offense close reasons from the **Admin** tab.

### Adding a custom offense close reason

When you add a custom offense close reason, the new reason is listed on the **Custom Close Reasons** window and in the **Reason for Closing** list box on the **Close Offense** window of the **Offenses** tab.

#### Procedure


1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.
3. Click **Add**.
4. Type a unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
5. Click **OK**.

Your new custom offense close reason is now listed in the **Custom Close Reasons** window. The **Reason for Closing** list box on the **Close Offense** window of the **Offenses** tab also displays the custom reason that you added.

### Editing custom offense close reason

Editing a custom offense close reason updates the reason in the **Custom Close Reasons** window and the **Reason for Closing** list box on the **Close Offense** window of the **Offenses** tab.


#### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.
3. Select the offense close reason that you want to edit.
4. Click **Edit**.
5. Type a new unique reason for closing offenses. Reasons must be between 5 and 60 characters in length.
6. Click **OK**.

## Deleting a custom offense close reason

Deleting a custom offense close reason removes the reason from the **Custom Close Reasons** window and the **Reason for Closing** list box on the **Close Offense** window of the **Offenses** tab.

### Procedure


1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Custom Offense Close Reasons**.
3. Select the offense close reason that you want to delete.
4. Click **Delete**.
5. Click **OK**.

## Configuring a custom asset property

---

Custom asset properties provide more query options when you run queries on the assets that you have in IBM QRadar.

### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Custom Asset Properties**.
3. In the **Name** field, enter a descriptor for the custom asset property.  
**Note:** The name must contain only alphanumeric characters, spaces, or underscores. No special characters are allowed.
4. In the **Type** list, select **Numeric** or **Text** to define the information type for the custom asset property.
5. Click **OK**.
6. Click the **Assets** tab.
7. Click **Edit Asset > Custom Asset Properties**.
8. Enter the required information in the value field.
9. Click **OK**.

## Adding custom actions

---

Attach scripts to custom rules to do specific actions in response to network events. Use the **Custom Action** window to manage custom action scripts.


Use custom actions to select or define the value that is passed to the script and the resulting action.

For example, you can write a script to create a firewall rule that blocks a source IP address from your network in response to a rule that is triggered by a defined number of failed login attempts.

The following examples are custom actions that are the outcomes of passing values to a script:

- Block users and domains.
- Initiate work flows and updates in external systems.
- Update TAXI servers with a STIX representation of a threat.

Custom actions work best with low volume custom rule events and with custom rules that have a low response limiter value.

1. On the navigation menu (  ), click **Admin**.
2. In the **Custom Actions** section, click **Define Actions**.
3. To upload your scripts, click **Add**. Programming language versions that the product supports are listed in the **Interpreter** list.

For the security of your deployment, QRadar does not support the full range of scripting functionality that is provided by the Python, Perl, or Bash languages.

4. Specify the parameters that you want to pass to the script that you uploaded.

| Table 8. Custom action parameters |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                         | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Fixed property</b>             | Values that are passed to the custom action script.<br><br>These properties are not based on the events or flow themselves, but cover other defined values that you can use the script to act on. For example, pass the fixed properties <b>username</b> and <b>password</b> for a third-party system to a script to send an SMS alert.<br><br>Encrypt fixed properties by selecting the <b>Encrypt value</b> check box. |
| <b>Network event property</b>     | Dynamic Ariel properties that are generated by events. Select from the <b>Property</b> list.<br><br>For example, the network event property <b>sourceip</b> provides a parameter that matches the source IP address of the triggered event.<br><br>For more information about Ariel properties, see the <i>IBM QRadar Ariel Query Language Guide</i> .                                                                   |

Parameters are passed into your script in the order in which you added them in the **Custom Actions** window.

When custom action scripts are run, a `chroot jail` is set up in the `/opt/qradar/bin/ca_jail/` directory. Any content in the `/opt/qradar/bin/ca_jail/` directory can be modified and written to by scripts. The custom action user's home directory (`/home/customactionuser`) can also be modified.

A script can run only from inside the jail environment so that it does not interfere with the QRadar run environment. All file access during custom action execution is relative to the `/opt/qradar/bin/ca_jail/` directory.

The custom action user account might not have permission to run follow-up commands, such as logging into a firewall and blocking an IP address. Test whether your script runs successfully before you associate it with a rule.

**Note:** The type of custom action that you implement depends on your network infrastructure and its components. For example, you can configure REST APIs on Cisco devices to block suspect IP addresses. Other third-party vendors might not provide a REST interface, so you might need to develop your own web services solution to run custom actions.

You must run the `dos2unix` utility on scripts that originate from a Windows or DOS system. Windows or DOS systems typically add control characters. To successfully test custom action scripts by using the script **Test Execution** function in QRadar, you must remove the control characters.

#### Related information

[Introduction to Custom Action Scripts](#)

## Testing your custom action

Test whether your script runs successfully and has the intended result before you associate it with a rule.

### About this task

Custom action scripts run inside a testing environment that is isolated from your production environment. Custom action scripts typically run on the managed host that runs the event processor. However, if you have an All-In-One appliance, custom actions run on the QRadar Console.

**Test Execution** is supported only on the QRadar Console and is not supported on managed hosts.

If you must write to disk from a custom action script, you must use the following directory: `/home/customactionuser`.

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Custom actions** section, click **Define actions**.
3. Select a custom action from the list and click **Test Execution > Execute** to test your script. The result of the test and any output that is produced by the script is returned.
4. After you configure and test your custom action, use the **Rule Wizard** to create a new event rule and associate the custom action with it.

For more information about event rules, see the *IBM QRadar User Guide*.

## Related information

[How do I configure rule actions in ? \(Security Learning Academy course\)](#)

## Passing parameters to a custom action script

Sample scripts in Bash, Python, and Perl show how to pass parameters to custom action scripts.

The following simple sample scripts show how to query the asset model API for an asset with the supplied offense source IP address. For the sake of this example, the scripts output the JSON that is returned by the endpoint.

The scripts require three parameters:

- Console IP address
- API token
- Offense source IP address

These parameters are configured in the Define Custom Action window **Script Parameters** area:

| Name              | Type                   | Value                                |
|-------------------|------------------------|--------------------------------------|
| console_ip        | Fixed Property         |                                      |
| api_token         | Fixed Property         | 4e176ca6-a46a-3471-8211-45f3d7f2893e |
| offense_source_ip | Network Event Property | sourceip                             |

Figure 6. Custom action script parameters



Each parameter is passed to the script in the order in which it was added in the Define Custom Action window. In this case:

1. console\_ip
2. api\_token
3. offense\_source\_ip

The variables that are defined at the beginning of each of the sample scripts use the sample parameter names that were added in the Define Custom Action window.

```
#!/bin/bash
console_ip=$1
api_token=$2
offense_source_ip=$3

auth_header="SEC:$api_token"

output=$(curl -k -H $auth_header https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29)

Basic print out of the output of the command
echo $output
```

Figure 7. *call\_asset\_model.sh*

```
#!/usr/bin/python
import sys
import requests
console_ip = sys.argv[1]
api_token = sys.argv[2]
offense_source_ip = sys.argv[3]

auth_header = {'SEC' : api_token }

endpoint = "https://{0}/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22%22%22%29%29"
.format(console_ip, offense_source_ip)

response = requests.get(endpoint, headers=auth_header, verify=False)

Basic print out of the output of the command
print(response.json())
```

Figure 8. *call\_asset\_model.py*

```
#!/usr/bin/perl
use strict;
use warnings;
use LWP::UserAgent;

my $console_ip = $ARGV[0];
my $api_token = $ARGV[1];
my $offense_source_ip = $ARGV[2];

my $endpoint = "https://$console_ip/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29";

my $client = LWP::UserAgent -> new(ssl_opts => { verify_hostname => 0 });

my $response = $client -> get($endpoint, "SEC" => $api_token);

Basic print out of the output of the command
print $response -> decoded_content;
```

Figure 9. *call\_asset\_model.pl*

## Managing aggregated data views

A large volume of data aggregation can decrease your system performance. The Ariel function uses a separate database for aggregated data in order to improve system performance and to make the data more readily available. You can disable, enable, or delete aggregated data views. Time series charts, report charts, and anomaly rules use aggregated data views.

### About this task

The items that appear in the **Display** list sort the data.

The Aggregated Data View is required to generate data for ADE rules, time series graphs, and reports.

Disable or delete views if the maximum number of views is reached.

Duplicate views can appear in the **Aggregated Data ID** column because an aggregated data view can include multiple searches.

### Procedure


1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Aggregated Data Management**.
3. To filter the list of aggregated data views, perform one the following options:
  - Select an option from the **View**, **Database**, **Show**, or **Display** list.
  - Type an aggregated data ID, report name, chart name, or saved search name in the search field.
4. To manage an aggregated data view, select the view, and then click the appropriate action on the toolbar:
  - If you select **Disable View** or **Delete View**, content dependencies are displayed for the aggregated data view. After you disable or delete the view, the dependent components no longer use aggregated data.
  - Enable a previously disabled aggregated data view to restore the view.

Table 9. Aggregated Data Management View column descriptions

| Column               | Description                                                                                                   |
|----------------------|---------------------------------------------------------------------------------------------------------------|
| Aggregated Data ID   | Identifier for the aggregated data                                                                            |
| Saved Search Name    | Defined name for the saved search                                                                             |
| Column Name          | Column identifier                                                                                             |
| Times Searches       | Search count                                                                                                  |
| Data Written         | The size of the written data                                                                                  |
| Database Name        | Database where the file was written                                                                           |
| Last Modified Time   | Timestamp of the last data modification                                                                       |
| Unique Count Enabled | True or False: Search the results to display unique event and flowcounts instead of average counts over time. |

---

## Chapter 6. Event data processing in QRadar

In IBM QRadar, use the DSM Editor to solve parsing problems and to add custom parsing.

The DSM Editor provides real-time feedback so that you know whether your customization works the way that you expect it to.

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## DSM Editor overview

Instead of manually creating a log source extension to fix parsing issues or extend support for new log source types, use the DSM Editor. The DSM Editor provides different views of your data. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definition.

The DSM Editor provides the following views:

### Workspace

The **Workspace** shows you raw event data. Use sample event payloads to test the behavior of the log source type, and then the **Workspace** area shows you the data that you capture in real time.

All sample events are sent from the workspace to the DSM simulator, where properties are parsed and QID maps are looked up. The results are displayed in the **Log Activity Preview** section. Click the edit icon to open in edit mode.

In the edit mode, you paste up to 100,000 characters of event data into the workspace or edit data directly. When you edit properties on the **Properties** tab, matches in the payload are highlighted in the workspace. Custom properties and overridden system properties are also highlighted in the **Workspace**.

New in 7.4.1 You can specify a custom delimiter that makes it easier for QRadar to ingest multiline events. To ensure that your event is kept intact as a single multiline event, select the **Override event delimiter** checkbox to separate the individual events based on another character or sequence of characters. For example, if your configuration is ingesting multiline events, you can add a special character to the end of each distinct event in the **Workspace**, and then identify this special character as the event delimiter.

### Log activity preview

New in 7.4.1 The **Parsing Status** column was added to the Log Activity Preview.

The **Log Activity Preview** simulates how the payloads in the workspace appear in the **Log Activity** viewer. The **Parsing Status** column indicates whether your event properties are successfully parsing and mapping to a QID record. Every standard property that is supported is displayed. The fields that are marked with an asterisk (\*), for example, **Event name**, **Severity**, **Low-level category**, and **QID**, are populated from the QID map. Fields that are populated from the QID map cannot be parsed verbatim from the raw events data in the workspace, so they cannot be defined or edited. You can adjust their values by selecting the corresponding event ID and category combination from the **Event Mappings** tab. Then click **Edit** to re-map an event to a different QID record that exists in the system or to a newly created QID.

**Important:** You must set an **Event ID** for any system properties to be parsed correctly.

Click the configure icon to select which columns to show or to hide in the **Log Activity Preview** window, and to reorder the columns.

## Properties

The **Properties** tab contains the combined set of system and custom properties that constitute a DSM configuration. Configuring a system property differs from configuring a custom property. You can override a property, by selecting the **Override system behaviour** check box and defining the expression.

**Note:** If you override the **Event Category** property, you must also override the **Event ID** property.

Matches in the payload are highlighted in the event data in the workspace. The highlighting color is two-toned, depending on what you capture. For example, the orange highlighting represents the capture group value while the bright yellow highlighting represents the rest of the regex that you specified. The feedback in the workspace shows whether you have the correct regex. If an expression is in focus, the highlighting in the workspace reflects only what that expression can match. If the overall property is in focus, then the highlighting turns green and shows what the aggregate set of expressions can match, taking into account the order of precedence.

In the **Format String** field, capture groups are represented by using the  $\$<number>$  notation. For example,  $\$1$  represents the first capture group from the regex,  $\$2$  is the second capture group, and so on.

You can add multiple expressions to the same property, and you can assign precedence by dragging and dropping the expressions to the top of the list.

A warning icon beside any of the properties indicates that no expression was added.

## Event mappings tab

New in 7.4.1 Support for copying Event ID and Event Category fields was added to the **Event Mapping** tab.

The **Event Mappings** tab displays all the event ID and category combinations that exist in the system for a selected log source type. If a new event mapping is created, it is added to the list of event ID and category combination that is displayed in the **Event Mappings** tab. In general, the **Event Mappings** tab displays all event ID and category combinations and the QID records that they are mapped to.

## Configuration tab

You can configure Auto Property Discovery for structured data that are in JSON format. By default, log source types have Auto Property Discovery turned off.

When you enable **Auto Property Discovery** on the **Configuration** tab, the property discovery engine automatically generates new properties to capture all fields that are present in the events that are received by a log source type. You can configure the number of consecutive events to be inspected for new properties in the **Discovery Completion Threshold** field. Newly discovered properties appear in the **Properties** tab, and are made available for use in the rules and search indexes. However, if no new properties are discovered before the threshold, the discovery process is considered complete and **Auto Property Discovery** for that log source type is disabled. You can manually enable the Auto Property Discovery on the Configuration tab at any time.

**Note:** To continuously inspect events for a log source type, you must make sure that you set the **Discovery Completion Threshold** value to 0.

### Related concepts

[Properties in the DSM Editor](#)

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

## Properties in the DSM Editor

---

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

A DSM cannot have multiple properties with the same name.

The configuration of a system property differs from a custom property.

## System properties

System properties cannot be deleted but you can override the default behavior. There are two types of system properties:

### Predefined system property

Displays the default QRadar behavior that is used for the DSM.

### Override system property

System properties with override configured (log source extension) show **Override** in the status line. When a system property has an override, a log source extension for that DSM uses the regular expressions that you entered for the configuration.

## Custom properties

Custom properties show **Custom** in the status line.

Custom properties differ from system properties in these ways:

- Custom properties display **Custom** below their name.
- Custom properties have no **Override system behavior** check box.
- To make a custom property available for rules and search indexing, select the **Enable this Property for use in Rules and Search Indexing** check box when you create a custom property.

**Note:** When you select this option, QRadar attempts to extract the property from events as soon as they enter the pipeline. Extracted property information and the remainder of the event record are persisted. The property does not need to be extracted again when it is used in a search, or report. The process enhances performance when the property is retrieved, but the process can have a negative impact on performance during event collection and storage.

- Custom properties must have one or more expressions to be valid.

### Related concepts

[DSM Editor overview](#)

Instead of manually creating a log source extension to fix parsing issues or extend support for new log source types, use the DSM Editor. The DSM Editor provides different views of your data. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definition.

[Custom property definitions in the DSM Editor](#)

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

## Property configuration in the DSM Editor

---

Configure properties in the DSM Editor to change the behavior of an overridden system property or the custom property of a DSM.

When you override the behavior of a system property, you must provide a valid expression on the **Properties** tab. The **Format String** field is a combination of regex capture groups and literal characters. The string is used to populate system properties by one or more values that are captured from events, and with more formatting characters or injected information. For example, you might want to parse an IP address and a port to combine them both into a string. If your regular expression (regex) has two capture groups, you can combine them by using this format string: \$1:\$2.



**Attention:** The DSM Editor allows capture group references of 1 through 9 in any specific match. If you reference any capture group above 9, the log source extension might not work correctly.

You must configure each custom property that you create. You must provide a valid expression and capture group for a custom property on the **Properties** tab. You can also define selectivity and enable or disable your expression.

### Related concepts

[“Custom property definitions in the DSM Editor” on page 64](#)

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

## Referencing capture strings by using format string fields

Use the **Format String** field on the **Property Configuration** tab to reference capture groups that you defined in the regex. Capture groups are referenced in their order of precedence.

### About this task

A capture group is any regex that is enclosed within parenthesis. A capture group is referenced with an \$n notation, where n is a group number that contains a regular expression (regex). You can define multiple capture groups.

For example, you have a payload with company and host name variables.

```
"company": "ibm", "hostname": "localhost.com"
"company": "ibm", "hostname": "johndoe.com"
```

You can customize the host name from the payload to display *ibm.hostname.com* by using capture groups.

### Procedure

1. In the **regex** field, enter the following regular expression:  
"company": "(.\*)".\*"hostname": "(.\*)"
2. In the **Format String** field, enter the capture group \$1.\$2 where \$1 is the value for the company variable (in this case ibm) and \$2 is the value for the host name in the payload. The following output is given:  
ibm.localhost.com ibm.johndoe.com

## Regex for well-structured logs

Well-structured logs are a style of event formatting that is composed of a set of properties and are presented in the following way:

```
<name_of_property_1><assignment_character>
<value_of_property_1><delimiter_character>
<name_of_property_2><assignment_character>
<value_of_property_2><delimiter_character>
<name_of_property_3><assignment_character>
<value_of_property_3><delimiter_character>...
```

Use the following general guidelines:

- The **<assignment\_character>** either '=' or ':' or a multi-character sequence such as '->'.
- The **<delimiter\_character>** either a white space character (space or tab) or a list delimiter, such as a comma or semi-colon.
- The **<value\_of\_property>** and sometimes **<name\_of\_property>** are encapsulated in quotation marks or other wrapping characters.

For example, consider a simple login event that is generated by a device or an application. The device might report on the account of a user who logged in, the time the login occurred, and the IP address of the computer from which the user logged in. A name/value pair-style event might look like this snippet:

```
<13>Sep 09 22:40:40 192.0.2.12 action=login accountname=JohnDoe clientIP=192.0.2.24
timestamp=01/09/2016 22:40:39 UTC
```

**Note:** The string "<13>Sep 09 22:40:40 192.0.2.12" is a syslog header. The string is not part of the event body.

The following table shows how the properties of the well-structured log example above, can be captured:

| Table 10. Regex for capturing properties of a well-structured log |                     |
|-------------------------------------------------------------------|---------------------|
| Property                                                          | Regex               |
| action                                                            | action=(.*?)\t      |
| accountname                                                       | accountname=(.*?)\t |
| clientIP                                                          | clientIP=(.*?)\t    |
| timestamp                                                         | timestamp=(.*?)\t   |

The patterns that are enclosed within the brackets denote the capture group. Each regex in the table captures everything after the equal sign (=) and before the next tab character.

## Regex for natural language logs

Natural language logs are presented in a sentence-like form and each event type might look different.

For example, a simple login event can be presented in the following form:

```
<13>Sep 09 22:40:40 192.0.2.12 Account JohnDoe initiated a login action
from 192.0.2.24 at 01/09/2016 22:40:39 UTC
```

The following table shows how the properties of the natural language log in the example above, can be captured:

| Table 11. Regex for capturing properties of a natural language log |                          |
|--------------------------------------------------------------------|--------------------------|
| Property                                                           | Regex                    |
| action                                                             | initiated a (.*?) action |
| accountname                                                        | Account (.*?) initiated  |
| clientIP                                                           | from (.*?) at            |
| timestamp                                                          | at (.*?)                 |

**Note:** Writing regex for natural language logs requires you to look at the static information that surrounds the value you want to capture before you create the capture group.

## Expressions in JSON format for structured data

Structured data in JSON format contains one or more properties, which are represented as a key-value pair.

### About this task

You can extract properties from event data that is presented in JSON format by writing a JSON expression that matches the property. The JSON expression must be a path in the format of */"<name of top-level field>"*.

For example, you have event data that is formatted in JSON:

```
{ "action": "login", "user": "John Doe" }
```

or an event that has a nested JSON format, such as:

```
{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }
```

## Procedure

To extract properties from event data, choose one of the following methods:

- To extract the 'user' property for event data that is formatted in JSON, type the expression `/"user"` in the **Expression** field.
- To extract the 'last\_name' of the user for an event that has a nested JSON format, type the expression `/"user"/"last_name"` in the **Expression** field.

## JSON keypath expressions

To uniquely identify the fields that you want to extract from a JSON object, your JSON expression must follow specific JSON keypath conventions.

Use the following guidelines for your JSON keypath expressions:

- A forward slash (/) must be at the start of all JSON keypaths. All paths must start at the beginning of the root JSON object. Subsequent slashes in the keypath indicate access to fields that are nested in the JSON object.
- Field names must be enclosed in double quotation marks.

A valid path might look like the following example:

```
/"object"/"nestedObject"/"furtherNestedObject"/"desiredPropertyName"
```

- Square brackets indicate the handling of JSON arrays.

If you do not supply an index in the square brackets, the entire body of the array is extracted. If you supply an index in the square bracket, that index in the array is extracted or nested. Arrays begin at a zero index, where 0 is the first index in the array, 1 is the second index in the array, and so on.

In the following keypath example, the JSON parser looks into the second index of the "object" JSON array, and then within that array index, looks for a field called "desiredPropertyName".

```
/"object"[1]/"desiredPropertyName"
```

- Within log source extensions, you can supply and combine together multiple JSON keypaths to give a single result; this convention excludes custom properties. You can also choose to include literal text. Each of the JSON keypaths must be enclosed in curly braces.

Consider the following example:

```
{/"object"/"nestedObject"/"desiredPropertyName1"} {/"object"/"nestedObject"/"desiredPropertyName2"}
```

You get a parsed value from the first JSON keypath, a literal text space, and then a parsed value from the second JSON keypath.

**Example:** The following two examples show how to extract data from a JSON object:

- Simple case of a JSON object:

```
[{"name":"object1","field1":"value1"}, {"name":"object2","field2":"value2"}, {"name":"object3","field3":"value3"}]
```

The following table shows the values that are extractable from the keypaths in that sample object:



Table 12. Keypaths from the simple JSON object

| Keypaths    | Description                                                                                                | Value                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| /[]         | Extracts the entire JSON array from the root of the JSON object.                                           | [{"name":"object1","field1":"value1"}, {"name":"object2","field2":"value2"}, {"name":"object3","field3":"value3"}] |
| /[1]/"name" | Extracts the value for the attribute called "name" from the JSON object at index 1 in the root JSON array. | object2                                                                                                            |

- Complex case of a JSON object:

```
<13>May 22 10:15:41 log.test.com {"module":"CPHalo","version":"1.0","user_name":"user123",
"event_type":"File integrity scan request created",
"event_category":"File Integrity Scanning Management","srcName":"domain-lab-123",
"timestamp":"2018-12-02T15:36:17.486","user":
{"email":"user123@example.com","first_name":"fname",
"last_name":"lname","alias":["alias name","alias1","name"]},"client_ip":"12.12.12.12",
"server_id":"12317412471421274","server_reported_fqdn":"None","actor_country":"USA",
"server_group_name":"Example Server","server_platform":"Linux",
"message":"A file integrity monitoring scan was requested for Linux server domain-lab-123
(13.13.13.13) by Halo user user123@example.com from IP address 12.12.12.12 (USA).",
"type":"fim_scan_request_created","id":"c2e8bf72-b74f-11e2-9055-870a490fcfb6"}
```

The following table shows the values that are extractable from the keypaths in that sample object:

Table 13. Keypaths from the complex JSON object

| Keypaths                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                 | Value                          |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| /"user_name"                                      | Extracts value of the "user_name" attribute from the root of the JSON object.                                                                                                                                                                                                                                                                                                                               | user123                        |
| /"user"/"alias"[]                                 | Extracts the entire JSON array called "alias" that is nested under the "user" JSON object.                                                                                                                                                                                                                                                                                                                  | ["alias name","alias1","name"] |
| /"user"/"alias"[0]                                | Extracts the value at index 0 within the "alias" JSON array that is nested under the "user" JSON Object.                                                                                                                                                                                                                                                                                                    | alias name                     |
| /"user"/"first_name"                              | Extracts the value of the property called "first_name" that is nested under the "user" JSON Object.                                                                                                                                                                                                                                                                                                         | fname                          |
| {/"user"/"first_name"}.<br>{/ "user"/"last_name"} | Extracts the value of the property called "first_name" that is nested under the "user" JSON object, then inserts a literal '.' character, and then extracts the value of the property called "second_name" that is nested under the "user" JSON object.<br><br>Pertains only to log source extensions and non-custom properties within the DSM Editor. This operation is not possible in custom properties. | fname.lname                    |

| Table 13. Keypaths from the complex JSON object (continued) |                                                                                                                                                                                                                                                                                                                                                                                             |                    |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Keypaths                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                 | Value              |
| <code>/{ "user"/"alias"[1]}@/{ "client_ip"}</code>          | <p>Extracts the value at index 1 of the "alias" JSON array that is nested under the "user" JSON object, inserts a literal '@' character, and then extracts the value of the property called "client_ip" under the root JSON object.</p> <p>Pertains only to log source extensions and non-custom properties within the DSM Editor. This operation is not possible in custom properties.</p> | alias1@12.12.12.12 |

## Expressions in LEEF format for structured data

Structured data in LEEF format contains one or more properties, which are represented as key-value pairs.

### About this task

You can extract properties from an event that is presented in LEEF format by writing a LEEF expression that matches the property. Valid LEEF expressions are in the form of either a single key reference, or a special LEEF header field reference.

For example, you have an event that is formatted in LEEF V1.0, such as:

```
LEEF:1.0|ABC Company|SystemDefender|1.13|console_login|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
devTime=2017-10-18T11:26:03.060+0200 usrName=flastname name=Firstname Lastname
authType=interactivePassword src=192.168.0.1
```

or an event that is formatted in LEEF V2.0 with the caret (^) separator character, such as:

```
LEEF:2.0|ABC Company|SystemDefender|1.13|console_login|^|devTimeFormat=yyyy-MMdd'T'HH:mm:ss.SSSZ^
devTime=2017-10-18T11:26:03.060+0200^usrName=flastname^name=Firstname Lastname
^authType=interactivePassword^src=192.168.0.1
```

You can extract a property or a header key property from the event by choosing one of the following methods:

### Procedure

1. To extract the 'usrName' property, enter `usrName` in the **LEEF Key** field.

The possible keys that can be extracted are:

- devTimeFormat
- devTime
- usrName
- name
- authType
- src

2. To extract a header key property, type the key in the following format in the **LEEF Key** field:

```
$eventid$
```

The LEEF header values can be extracted by using the following expressions:

- \$leefversion\$
- \$vendor\$
- \$product\$
- \$version\$
- \$eventid\$

## Expressions in CEF format for structured data

Structured data in CEF format contains one or more properties, which are represented as key-value pairs.

### About this task

You can extract properties from an event that is presented in CEF format by writing a CEF expression that matches the property. Valid CEF expressions are in the form of either a single key reference, or a special CEF header field reference.

For example, you have an event that is formatted in CEF:

```
CEF:0|ABC Company|SystemDefender|1.13|console_login|Console Login|1|start=Oct 18 2017 11:26:03
duser=jsmith cs1=John Smith cs1Label=Person Name cs2=interactivePassword cs2Label=authType
src=1.1.1.1
```

You can extract a property or a header key property from the event by choosing one of the following methods:

### Procedure

1. To extract the 'cs1' property, type cs1 in the **CEF Key** field.

The possible keys that can be extracted are:

- start
- duser
- cs1
- cs1Label
- cs2
- cs2Label
- src

2. To extract a header key property, type the key in the following format in the **CEF Key** field:

```
id
```

The CEF header values can be extracted by using the following expressions:

- \$cefversion\$
- \$vendor\$
- \$product\$
- \$version\$
- \$id\$
- \$name\$
- \$severity\$

## Expressions in Name Value Pair format for structured data

Structured data in Name Value Pair format contains one or more properties, which are represented as key-value pairs.

### About this task

You can extract properties from an event that is in Name Value Pair format by writing an expression that matches the property. Valid Name Value Pair expressions are in the form of a single key reference.

The following example shows an event that is in Name Value Pair format:

```
Company=ABC
Company;Product=SystemDefender;Version=1.13;EventID=console_login;Username=jsmith;Name=John
Smith;authType=interactivePassword;
```

### Procedure

1. To extract the Username property, type Username in the **Expression** field.
2. In the **Value Delimiter** field, enter the key-value delimiter that is specific for your payload. In this example, the key-value delimiter is an equal sign (=).
3. In the **Delimiter** field, enter the delimiter between key-value pairs that is specific for your payload. In this example, the delimiter between key-value pairs is a semicolon (;).

### Results

Matches in the payload are highlighted in the event data in the **Workspace** of the DSM Editor.

## Expressions in Generic List format for structured data

Structured data in Generic List format contains one or more properties, which are represented as list items.

### About this task

You can extract properties from an event that is in Generic List format by writing an expression that matches the property. Valid Generic List expressions are in the form of a  $\$<number>$  notation. For example, \$0 represents the first property in the list, \$1 is the second property, and so on.

The following example shows an event that is in Generic List format:

```
ABC Company;1.13;console_login;jsmith;John Smith;interactivePassword;
```

### Procedure

1. To extract the first property in the list, type \$0 in the **Expression** field.
2. In the **Delimiter** field, enter the delimiter between list items that is specific for your payload. In this example, the delimiter between list items is a semicolon (;).

### Results

Matches in the payload are highlighted in the event data in the **Workspace** of the DSM Editor.

## Expressions in XML format for structured data

Structured data in XML format contains one or more properties, which are represented as key-value pairs.

You can extract properties from an event that is in XML format by writing an expression that matches the property. Valid XML expressions are in the form of a single key reference.

Enter the path to the XML field that you want to use to populate the property's value. An XML key path must begin with a forward slash (/) to indicate the root of the XML object, and be followed by one or more XML field names within double quotation marks.

The following example shows an event that is in XML format:

```
<EPOEvent><MachineInfo><MachineName>NEPTUNE</MachineName><MachineName>VALUE23</MachineName><AgentGUID>9B-B5-A6-A8-37-B3</AgentGUID><IPAddress someattrib="someattribvalue">192.0.2.0</IPAddress><OSName>Windows 7</OSName><UserName>I am a test user</UserName></MachineInfo></EPOEvent>
```

To capture the value nested in the top-level OSName object, type `/"EPOEvent"/"MachineInfo"/"OSName"` in the **Expression** field.

To capture the attribute value, use a period (.) after the key path. For example, to capture `someattribvalue`, type `/"EPOEvent"/"MachineInfo"/"IPAddress".someattrib` in the **Expression** field.

To combine multiple fields together with multiple paths, use set brackets to enclose each. For example, `{/"EPOEvent"/"MachineInfo"/"OSName"}`  
`{/"EPOEvent"/"MachineInfo"/"MachineName"[1]}`


To capture the value that is nested within multiple tags with the same name, use `[0]`, `[1]`, and so on, after the key path. For example, to capture `VALUE23`, type `/"EPOEvent"/"MachineInfo"/"MachineName"[1]` in the **Expression** field.

Matches in the payload are highlighted in the event data in the **Workspace** of the DSM Editor.

## Opening the DSM Editor

You can open the DSM Editor from the **Log activity** tab, or if you are an administrator, you can open it from the **Admin** tab. For example, if events that are sent to the system are not handled properly, you can select the event data from the **Log Activity** tab and send it to the DSM Editor. For events that are not yet sent to the system, you must be an administrator and access the DSM Editor from the **Admin** tab.

### Procedure

1. To open the DSM Editor from the **Admin** tab, follow these steps:
  - a) On the navigation menu () , click **Admin**.
  - b) In the **Data Sources** section, click **DSM Editor**.
2. To open the DSM Editor from the **Log Activity** tab, follow these steps:
  - a) Click the **Log Activity** tab.
  - b) Pause the incoming results and then highlight one or more events.


**Important:** If more than one event from two or more log sources are selected, you are prompted to select which log source type you want to operate on. You can select only a single log source type, and only the events from log activity that match the selected log source type are automatically added to the workspace.

- c) On the navigation menu, select **Actions > DSM Editor**

## Configuring a log source type

With the DSM Editor, you can configure a new log source type or use an existing one in IBM QRadar.

### Procedure

1. On the navigation menu () , click **Admin**.
2. In the **Data Sources** section, click **DSM Editor**.
3. Create a log source type or select an existing log source type:

- To create a new log source type, click **Create New** and follow the prompts.
- To locate an existing log source type, use the **Filter** field and then click **Select**.

## Configuring property autodetection for log source types

---

When you enable **Property Autodetection**, new properties are automatically generated to capture all fields that are in the events that the selected log source type receives. Configure property autodetection of new properties for a log source type so that you do not need to manually create a custom property for each instance.

### About this task

By default, **Property Autodetection** for a log source type is disabled.

### Procedure

1. In the DSM Editor, select a log source type or create a new one from the **Select Log Source Type** page.
2. Click the **Configuration** tab.
3. **Restriction:** Property autodetection works only for structured data that is in JSON, CEF, LEEF, or Name Value Pair format.

Click **Enable Property Autodetection**.

4. Select the structured data format for the log source type from the **Property Detection Format** list.  
If you choose **Name Value Pair**, in the **Delimiter In Name Value Pairs** section, enter the delimiter used to separate each name and value, and the delimiter used to separate each Name Value Pair. Delimiters for each pair are automatically created.
5. To enable new properties to use in rules and searches, click **Enable Properties for use in Rules and Search Indexing**.
6. In the **Autodetection Completion Threshold** field, set the number of consecutive events to inspect for new properties.  
If no new properties are discovered when the number of consecutive events are inspected, the discovery process is considered complete and **Property Autodetection** is disabled. You can manually re-enable **Property Autodetection** at any time. A threshold value of 0 means that the discovery process perpetually inspects events for the selected log source type.
7. Click **Save**.

### Results

The newly discovered properties appear in the **Properties** tab of the DSM Editor.

## Configuring Log Source Autodetection for Log Source types

---

Configure Log Source Autodetection for a log source type so that you don't need to manually create a log source for each instance. Log source autodetection configuration also helps to improve the accuracy of detecting devices that share a common format, and can improve pipeline performance by avoiding the creation of incorrectly detected devices.

### Before you begin

In QRadar V7.3.2, upgrades from previous versions enable global configuration settings, which are stored in the QRadar database. The global settings are initially set based on the contents of the `TrafficAnalysisConfig.xml` file in `/opt/qradar/conf/` directory on the QRadar Console. If this file was customized before you upgrade to V7.3.2, the customizations are preserved. If different customizations exist on other managed hosts in the deployment, these customizations aren't carried over to the global settings. You can still enable per-event processor autodetection settings by using the configuration file

method. Disable global autodetection settings in **Admin > System & License Management > Edit Managed Host > Component Management**.

## About this task

When Log Source Autodetection is enabled, if you create a custom log source type that has many instances in your network, you don't need to manually create a log source for each instance.

You can also use the QRadar REST API or a command line script to enable and disable which log source types are autodetected. If you use a smaller number of log source types, you can configure which log sources are autodetected to improve the speed of detection.

If you choose to revert to the file-based (non-global) settings, you can only configure autodetection by using the config file. The DSM Editor and REST API work only with global settings. Move any custom autodetection configurations to global settings and to the DSM Editor.

Tune the autodetection engine so that log sources aren't incorrectly identified as the wrong type. Incorrect detection happens when a DSM incorrectly recognizes events as its own even though they don't originate from the type of system that the DSM corresponds to. For example, if the events are formatted similarly to the events the DSM supports, or they contain the same keywords that the DSM is looking for. It can also happen even if a DSM exists for the system that is generating the events, if the events are so similar that the incorrect DSM is successful at parsing the events like the correct DSM. That DSM incorrectly recognizes the events as its own, and the autodetection engine creates a log source that isn't of the correct type.

For example, if you have both Linux® and AIX® systems in your QRadar deployment, and most of them are Linux. You can reduce the **Minimum Successful Events for Autodetection** parameter or the **Minimum Successful Events for Autodetection** for Linux. Alternatively, increase the **Minimum Successful Events for Autodetection** parameter or the **Minimum Successful Events for Autodetection** parameter for AIX.

## Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, click **DSM Editor**.
3. Select a log source type or create a new one from the **Select Log Source Type** window.
4. Click the **Configuration** tab, and then click **Enable Log Source Autodetection**.
5. Configure the following parameters:

| Parameter                              | Description                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log Source Name Template</b>        | Enter the template for setting the name of autodetected log sources.<br><br>Two variables can be used: <ul style="list-style-type: none"><li>• <b>\$\$DEVICE_TYPE\$\$</b> corresponds to the log source type name.</li><li>• <b>\$\$SOURCE_ADDRESS\$\$</b> corresponds to the source address the events originate from.</li></ul>        |
| <b>Log Source Description Template</b> | Enter the template for setting the description of autodetected log sources.<br><br>Two variables can be used: <ul style="list-style-type: none"><li>• <b>\$\$DEVICE_TYPE\$\$</b> corresponds to the log source type name.</li><li>• <b>\$\$SOURCE_ADDRESS\$\$</b> corresponds to the source address the events originate from.</li></ul> |

| Parameter                                          | Description                                                                                                      |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Minimum Successful Events for Autodetection</b> | The minimum number of events from an unknown source that must be successfully parsed for autodetection to occur. |
| <b>Minimum Success Rate for Autodetection</b>      | The minimum parsing success percentage for events from an unknown source for autodetection to occur.             |
| <b>Attempted Parse Limit</b>                       | The maximum number of events from an unknown source to attempt before abandoning autodetection.                  |
| <b>Consecutive Failed Parse Limit</b>              | The number of consecutive events from an unknown source to abandon autodetection.                                |

6. Click **Save**.

## Configuring DSM parameters for Log Source types

Use the DSM Editor to configure the DSM parameters for your log source type.

### About this task

If your log source type has DSM parameters, you can use the DSM Editor to edit the parameters.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, click **DSM Editor**.
3. Select a log source type or create a new one from the **Select Log Source Type** window.
4. Click the **Configuration** tab, and then click **Display DSM Parameters Configuration**.
5. Configure the parameters.  
The Default parameters apply to all instances of this DSM in your deployment which do not have an Event Collector-specific override. To set different parameter values for this DSM for a specific Event Collector, select it from the **Event Collector** list to override the Default settings.
6. Click **Save**.

## Custom log source types

Use the DSM Editor to create and configure a custom log source type to parse your events. If you create a log source type for your custom applications and systems that don't have a supported DSM, QRadar analyzes the data in the same way that it does for supported DSMs.

You can select events from the **Log Activity** tab and send them directly to the DSM Editor to be parsed. Or you can open the DSM Editor from the **Admin** tab to create and configure a new log source type.

Complete the fields in the DSM Editor with the correct structured data to parse relevant information from the events. QRadar uses the **Event Category** and **Event ID** fields to map a meaning to the event. The Event ID is a mandatory field that defines the event, and the category breaks down the event further. You can set the **Event Category** to the Device Type name, or you can leave it as unknown. If you leave the **Event Category** as unknown, you must set it to unknown for any event mappings that you create for this log source type.

Use the DSM Editor to map your Event ID/Event Category combinations that you are parsing from your events. Enter the Event ID/Event Category combination into the new entry in the **Event Mapping** tab. You can choose a categorization of the previously created QID map entry that is relevant to your event, or click **Choose QID** to create a new map entry.



## Related tasks

[“Creating an event map and categorization” on page 67](#)

An event mapping is an event ID and category combination you use to map an event to a QID. With the DSM Editor, you can create a new event mapping to map all unknown events to an entry in the QID map. Also, you can remap existing ones to either a newly created event categorization (QIDs) or to an existing one in the system.

## Creating a custom log source type to parse events

If you have events that are imported into QRadar, you can select the events on which you want to base your custom log source type and send them directly to the DSM Editor.

### Procedure

1. Click the **Log Activity** tab.
2. Pause the incoming results and then highlight one or more events.  
**Important:** You can select only a single log source type, and only the events from log activity that match the selected log source type are automatically added to the workspace.
3. On the navigation menu, select **Actions > DSM Editor**, and choose one of the following options:
  - If you are parsing known events, select your log source type from the list.
  - If you are parsing stored events, click **Create New**. Enter a name for your log source type in the **Log Source Type Name** field and click **Save**.
4. In the **Properties** tab, select the **Override system properties** checkbox for the properties that you want to edit.

### What to do next

[“Property configuration in the DSM Editor” on page 51](#)

## Related tasks

[“Creating an event map and categorization” on page 67](#)

An event mapping is an event ID and category combination you use to map an event to a QID. With the DSM Editor, you can create a new event mapping to map all unknown events to an entry in the QID map. Also, you can remap existing ones to either a newly created event categorization (QIDs) or to an existing one in the system.

[“Configuring property autodetection for log source types” on page 60](#)

When you enable **Property Autodetection**, new properties are automatically generated to capture all fields that are in the events that the selected log source type receives. Configure property autodetection of new properties for a log source type so that you do not need to manually create a custom property for each instance.

[“Configuring Log Source Autodetection for Log Source types” on page 60](#)

Configure Log Source Autodetection for a log source type so that you don't need to manually create a log source for each instance. Log source autodetection configuration also helps to improve the accuracy of detecting devices that share a common format, and can improve pipeline performance by avoiding the creation of incorrectly detected devices.

[“Creating a custom property” on page 64](#)

In the DSM Editor, you can define a custom property for one or more log source types whose events do not fit into the IBM QRadar normalized event model. For example, the set of system properties might not capture all relevant data from some applications, operating systems, databases, and other systems.

## Custom property definitions in the DSM Editor

---

You can define a custom property and reuse the same property in a separate DSM. Use these properties in searches, rules, and to allow specific user-defined behavior for parsing values into those fields.

Where relevant, each custom property has a set of configuration options that includes selectivity and data parsing. Each custom property definition within a DSM configuration is an ordered group of expressions that consists of an expression type, an expression, a capture group, an optional selectivity configuration, and an enabled or disabled toggle button. You can't modify the **Name**, **Field type**, **Description**, **optimize** fields, or any advanced options for a custom property on the **Properties** tab in the DSM Editor.

A custom property is shared across all DSMs, while specific implementations for reading values from payloads are at the DSM level.

Selectivity is specified when you configure an expression to run only when certain conditions are met.

**Note:** The **Capture Group** field of a custom property cannot be assigned a value greater than the number of capture groups in the regex.

### Related concepts

[Properties in the DSM Editor](#)

In the DSM Editor, normalized system properties are combined with custom properties and are sorted alphabetically.

## Selectivity

In the DSM Editor, you can restrict running a custom property to certain criteria for better performance.

The following are the types of restrictions:

### By high-level category and low-level category

A property is evaluated only when the high-level and low-level categories match a specific combination. For example, a property is evaluated only when the event is known to have a high-level category of **Authentication** and a low-level category of **Admin Logout**.

### By specific QID

A property is evaluated only when the event that is seen maps to a specific QID. For example, when the event maps to a QID of **Login Failed**, the property is evaluated.

## Expressions

You can define expressions for custom properties in the DSM Editor. Expressions are the mechanism that defines the behavior of a property. The main component of an expression is a valid regex or json. The data that makes up an expression depends on the property type.

For a custom property, you can choose only one capture group from the regex.

## Creating a custom property

In the DSM Editor, you can define a custom property for one or more log source types whose events do not fit into the IBM QRadar normalized event model. For example, the set of system properties might not capture all relevant data from some applications, operating systems, databases, and other systems.

### About this task

You can create custom property for data that does not fit into QRadar system properties. Use the custom properties in searches and test against them in rules.

| Table 14. Custom property parameters                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Name</b>                                                      | A descriptive name for the custom property that you create.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Field Type</b>                                                | <p>The default is <b>Text</b>.</p> <p><b>Note:</b> When you select <b>Number</b> or <b>Date</b> from the <b>Field Type</b> list, extra fields are displayed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Enable this Property for use in Rules and Search Indexing</b> | <p>When enabled, during the parsing stage of the event pipeline, QRadar attempts to extract the property from events immediately as they enter the system. Other components downstream in the pipeline such as rules, forwarding profiles and indexing can use the extracted values. Property information is persisted along with the rest of the event record and doesn't need to be extracted again when it is retrieved as part of a search or report. This option enhances performance when the property is retrieved, but can have a negative impact on performance during the event parsing process, and impacts storage.</p> <p>When not enabled, QRadar extracts the property from the events only when they are retrieved or viewed.</p> <p><b>Note:</b> For Custom Properties to be used in rule tests, forwarding profiles, or for search indexing, this check box must be selected because rule evaluation, event forwarding, and indexing occur before events are written to disk, so the values must be extracted at the parsing stage.</p> |
| <b>Use number format from a Locale</b>                           | This field displays when you select <b>Number</b> from the <b>Field Type</b> list. If you select the <b>Use number format from a Locale</b> check box, you must select an <b>Extracted Number Format</b> from the list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Extracted Date/Time Format</b>                                | <p>This field displays when you select <b>Date</b> from the <b>Field Type</b> list. You must provide a datetime pattern that matches how the datetime appears in the original event.</p> <p>For example, 'MMM dd YYYY HH:mm:ss' is a valid datetime pattern for a time stamp like 'Apr 17 2017 11:29:00'.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Locale</b>                                                    | <p>This field displays when you select <b>Date</b> from the <b>Field Type</b> list. You must select the locale of the event.</p> <p>For example, if the locale is <b>English</b>, it recognizes 'Apr' as a short form of the month 'April'. But if the event is presented in French and the month token is 'Avr' (for Avril), then set the locale to a <b>French</b> one, or the code does not recognize it as a valid date.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Procedure

1. To add a custom property, click **Add (+)** on the **Properties** tab in the DSM Editor.
2. To create a new custom property definition, use the following steps:
  - a) Select **Create New** on the **Choose a Custom Property Definition to Express** page.
  - b) On the **Create a new Custom Property Definition** page, enter values for the **Name**, **Field type**, and **Description** fields.

**Note:** When you select **Number** or **Date** from the **Field Type** list, extra fields display.
  - c) If you want to extract the property from events as they enter the system, select the **Enable this property for use in Rules and Search indexing** check box.
  - d) Click **Save**.
3. To use an existing custom property, use the following steps:
  - a) On the **Choose a Custom Property Definition to Express** page, search for an existing custom property from the **Filter Definitions** field.
  - b) Click **Select** to add the custom property.
4. To configure a custom property, use the following steps:
  - a) Locate and select the custom property on the **Properties** tab. Custom properties display the word **Custom** next to them to differentiate them from system properties.
  - b) Select an expression type from the **Expression Type** list.
  - c) Define a valid expression for the custom property based on the expression type that is selected in step b.

**Note:**

    - For Regex, the expression must be a valid java-compatible regular expression. Case-insensitive matching is supported only by using the (?i) token at the beginning of the expression. The (?i) token is saved in the log source extension .xml file. To use other expressions, such as (?s), manually edit the log source extension .xml file.
    - For JSON, the expression must be a path in the format of `/"<name of top-level field>"` with additional `/"<name of sub-field>"` to capture subfields if any.
    - For LEEF and CEF, to capture the value of a key/value pair, set the expression to the key. To capture the value of a header field, set the expression to the corresponding reserved word for that header field.
  - d) If the expression type is Regex, select a capture group.
  - e) Optional: To limit an expression to run against a specific category, click **Edit** to add selectivity to the custom property, and select a **High Level Category** and a **Low Level Category**.
  - f) Optional: To limit an expression to run against a specific event or QID, click **Choose Event** to search for a specific QID.
  - g) From the **Expression** window, click **Ok**.
5. To add multiple expressions and reorder them, follow these steps:
  - a) Click **Add (+)** at the top of the expressions list.
  - b) Drag expressions in the order that you want them to run.

## Related information

[Guidance on defining a datetime pattern](#)

## Event mapping

---

In the DSM Editor, the event mapping shows all the event ID and category combinations that are in the system.

An event mapping represents an association between an event ID and category combination and a QID record (referred to as event categorization). Event ID and category values are extracted by DSMs from events and are then used to look up the mapped event categorization or QID. Event categorizations store extra metadata for the event that might not exist verbatim in the raw event data, such as a human-readable name and description, a severity value, or a low level category assignment. Low-level categorization and severity are useful for search and rule definitions.



**Warning:** For multi-tenant environments, any user-defined mapping or event categorization information that is defined in the DSM Editor becomes visible across all tenants. You must ensure that no tenant-specific data is put in any event categorization names or descriptions.

### Creating an event map and categorization

An event mapping is an event ID and category combination you use to map an event to a QID. With the DSM Editor, you can create a new event mapping to map all unknown events to an entry in the QID map. Also, you can remap existing ones to either a newly created event categorization (QIDs) or to an existing one in the system.

#### Procedure

1. To add an event mapping, click the Add (+) icon on the **Event Mapping** tab of DSM Editor.
2. Ensure that values are entered for the **Event ID** and **Event Category** fields.
3. To create a new event categorization, use the following steps:
  - a) From the **Create a new Event Mapping** window, click **Choose QID**.
  - b) On the **QID Records** window, click **Create New QID Record**.
  - c) Enter values for the **Name**, **Description** fields, and select a **Log Source Type**, a **High Level Category**, a **Low Level Category**, and a **Severity**.
  - d) Click **Save** to create the new event categorization.
4. To use an existing event categorization, use the following steps:
  - a) From the **Create a new Event Mapping** window, click **Choose Event**.
  - b) Search for an existing event categorization on the **Event Categorizations** window.
  - c) Select a **High Level category**, **Low Level category**, **Log Source Type** or **QID**. Results are shown in the **Search Results** pane.
  - d) Click **Ok** to add the event category.



---

## Chapter 7. Using reference data in QRadar

Use reference data collections to store and manage business data that you want to correlate against the events and flows in your IBM QRadar environment. You can add business data or data from external sources into a reference data collection, and then use the data in QRadar searches, filters, rule test conditions, and rule responses.

Reference data collections are stored on the QRadar console, but the collections are regularly copied to each managed host. For best performance on data lookups, the managed host caches the most frequently referenced data values.

### External threat intelligence data

You can use reference data collections to integrate indicator of compromise (IOC) data from third-party vendors into QRadar. QRadar uses IOC data to detect suspicious behavior faster, which helps security analysts investigate threats and respond to incidents more quickly.

For example, you can import IOC data, such as IP addresses, DNS names, URLs, and MD5s, from open source or subscription-based threat data providers, and correlate it with events and incidents on your network.

### Business data

Reference data collections can contain business data that is specific to your organization, such as a list of users with privileged system access. Use the business data to create blacklists and whitelists.

For example, use a reference set that contains the user IDs of terminated employees to prevent them from logging in to the network. Or, you can use business data to build a whitelist that allows only a limited set of IP addresses to do specific functions.

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## Types of reference data collections

IBM QRadar has different types of reference data collections that can handle different levels of data complexity. The most common types are reference sets and reference maps.

If you want to use the same reference data in both QRadar SIEM and QRadar Risk Manager, use a reference set. You can't use other types of reference data collections with QRadar Risk Manager.

| Table 15. Types of reference data collections |                                |                                                                                                     |                                                                                                                                                 |
|-----------------------------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Type of collection                            | Description                    | How to use                                                                                          | Examples                                                                                                                                        |
| Reference set                                 | A collection of unique values. | Use a reference set to compare a property value against a list, such as IP addresses or user names. | To verify whether a login ID that was used to log in to QRadar is assigned to a user, create a reference set with the <b>LoginID</b> parameter. |

Table 15. Types of reference data collections (continued)

| Type of collection    | Description                                                                                                                                       | How to use                                                                                                                 | Examples                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reference map         | A collection of data that maps a unique key to a value.                                                                                           | Use a reference map to verify a unique combination of two property values.                                                 | To correlate user activity on your network, create a reference map that uses the <b>LoginID</b> parameter as a key, and the <b>Username</b> as a value.                                                                                        |
| Reference map of sets | A collection of data that maps a key to multiple values. Every key is unique and maps to one reference set.                                       | Use a reference map of sets to verify a combination of two property values against a list.                                 | To test for authorized access to a patent, create a map of sets that uses a custom event property for <b>Patent ID</b> as the key, and the <b>Username</b> parameter as the value. Use the map of sets to populate a list of authorized users. |
| Reference map of maps | A collection of data that maps one key to another key, which is then mapped to a single value. Every key is unique and maps to one reference map. | Use a reference map of maps to verify a combination of three property values.                                              | To test for network bandwidth violations, create a map of maps that uses the <b>Source IP</b> parameter as the first key, the <b>Application</b> parameter as the second key, and the <b>Total Bytes</b> parameter as the value.               |
| Reference table       | A collection of data that maps one key to another key, which is then mapped to a single value. The second key is assigned a data type.            | Use a reference table to verify a combination of three property values when one of the properties is a specific data type. | Create a reference table that stores <b>Username</b> as the first key, <b>Source IP</b> as the second key with an assigned <b>cidr</b> data type, and <b>Source Port</b> as the value.                                                         |

#### Related tasks

[“Creating reference data collections with the APIs” on page 75](#)

You can use the application program interface (API) to manage IBM QRadar reference data collections.

## Reference sets overview

Use reference sets in IBM QRadar to store data in a simple list format.

You can populate the reference set with external data, such as indicators of compromise (IOCs), or you can use it to store business data, such as IP addresses and user names, that is collected from events and flows that occur on your network.

A reference set contains unique values that you can use in searches, filters, rule test conditions, and rule responses. Use rules to test whether a reference set contains a data element, or configure the rule response to add data to a reference set. For example, you can create a rule that detects when an employee accesses a prohibited website, and configure the rule response to add the employee's IP address or user name to a reference set.



For more information about configuring rule responses to add data to a reference set, see the *IBM QRadar User Guide*.

### Related tasks

[Creating reference data collections with the APIs](#)

You can use the application program interface (API) to manage IBM QRadar reference data collections.

## Adding, editing, and deleting reference sets

Use a reference set to compare a property value, such as an IP address or user name, against a list. You can use reference sets with rules to keep watch lists. For example, you can create a rule to detect when an employee accesses a prohibited website and then add that employee's IP address to a reference set.

### About this task

After you add data to the reference set, the **Number of Elements** and **Associated Rules** parameters are automatically updated.

When you edit a reference set, you can change the data values, but you can't change the type of data that the reference set contains.

Before a reference set is deleted, QRadar runs a dependency check to see whether the reference set has rules that are associated with it.

**Note:** If you use techniques to obfuscate data on the event properties that you want to compare to the reference set data, use an alphanumeric reference set and add the obfuscated data values.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. To add a reference set:
  - a) Click **Add** and configure the parameters.

#### Learn more about reference set parameters:

The following table describes each of the parameters that are used to configure a reference set.

| Table 16. Reference Set parameters |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Name</b>                        | The maximum length of the reference set name is 255 characters.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Type</b>                        | <p>Select the data types for the reference elements. You can't edit the <b>Type</b> parameter after you create a reference set.</p> <p>The <b>IP</b> type stores IPv4 addresses. The <b>Alphanumeric (Ignore Case)</b> type automatically changes any alphanumeric value to lowercase.</p> <p>To compare obfuscated event and flow properties to the reference data, you must use an alphanumeric reference set.</p> |
| <b>Time to Live of elements</b>    | <p>Specifies when reference elements expire. If you select the <b>Lives Forever</b> default setting, the reference elements don't expire.</p> <p>If you specify an amount of time, indicate whether the time-to-live interval is based on when the data was first seen, or was last seen.</p> <p>QRadar removes expired elements from the reference set periodically (by default, every 5 minutes).</p>              |

| Table 16. Reference Set parameters (continued) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>When elements expire</b>                    | <p>Specifies how expired reference elements are logged in the <code>qradar.log</code> file when they are removed from the reference set.</p> <p>The <b>Log each element in a separate log entry</b> option triggers an <b>Expired ReferenceData element</b> log event for each reference element that is removed. The event contains the reference set name and the element value.</p> <p>The <b>Log elements in one log entry</b> option triggers one <b>Expired ReferenceData element</b> log event for all reference elements that are removed at the same time. The event contains the reference set name and the element values.</p> <p>The <b>Do not log elements</b> option does not trigger a log event for removed reference elements.</p> |

b) Click **Create**.

4. Click **Edit** or **Delete** to work with existing reference sets.

**Tip:** To delete multiple reference sets, use the **Quick Search** text box to search for the reference sets that you want to delete, and then click **Delete Listed**.

### Related tasks

[Viewing the contents of a reference set](#)

[Tracking expired user accounts](#)

Use reference data collections to identify stale data, such as expired user accounts, in your IBM QRadar environment.

## Viewing the contents of a reference set

View information about the data elements in the reference set, such as the domain assignment, the expiry on the data, and when the element was last seen in your network.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select a reference set and click **View Contents**.
4. Click the **Content** tab to view information about each data element.

**Tip:** Use the search field to filter for all elements that match a keyword. You can't search for data in the **Time To Live** column.

### Learn more about the data elements:

The following table describes the information that is shown for each data element in the reference set.

| Table 17. Information about the reference set data elements |                                                                                                                                                                                                                      |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                   | Description                                                                                                                                                                                                          |
| <b>Domain</b>                                               | Domain-specific reference data can be viewed by tenant users who have access to the domain, MSSP Administrators, and users who do not have a tenant assignment. Users in all tenants can view shared reference data. |
| <b>Value</b>                                                | The data element that is stored in the reference set. For example, the value might show user names or IP addresses.                                                                                                  |

| Table 17. Information about the reference set data elements (continued) |                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                                                               | Description                                                                                                                                                                                                             |
| <b>Origin</b>                                                           | Shows the user name when the data element is added manually, and the file name when the data was added by importing it from an external file. Shows the rule name when the data element is added in response to a rule. |
| <b>Time to Live</b>                                                     | The time that is remaining until this element is removed from the reference set.                                                                                                                                        |
| <b>Date Last Seen</b>                                                   | The date and time that this element was last detected on your network.                                                                                                                                                  |

- Click the **References** tab to view the rules that use the reference set in a rule test or in a rule response.

| Table 18. Content tab parameters |                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                        | Description                                                                                                                                            |
| <b>Rule Name</b>                 | Name of the rule that is configured to use the reference set.                                                                                          |
| <b>Group</b>                     | The group that the rule belongs to.                                                                                                                    |
| <b>Category</b>                  | Shows if the rule is a custom rule or an anomaly detection rule.                                                                                       |
| <b>Type</b>                      | Shows <b>event</b> , <b>flow</b> , <b>common</b> , or <b>offense</b> to indicate the type of data that the rule is tested against.                     |
| <b>Enabled</b>                   | A rule must be enabled for the custom rule engine to evaluate it.                                                                                      |
| <b>Response</b>                  | The responses that are configured for this rule.                                                                                                       |
| <b>Origin</b>                    | <b>System</b> indicates a default rule.<br><b>Modified</b> indicates that a default rule was customized.<br><b>User</b> indicates a user-created rule. |

- To view or edit an associated rule, double-click the rule in the **References** list and complete the rule wizard.

## Adding elements to a reference set

Add elements to a reference set when you want IBM QRadar to compare a property to the element value. Use QRadar to manually add elements to a reference set, or to import elements from a .csv file.

### Before you begin

To import elements, make sure that the .csv file is stored locally.

### About this task

You can assign reference data to a specific domain. Domain-specific reference data can be viewed by tenant users who have access to the domain, MSSP Administrators, and users who do not have a tenant assignment. Users in all tenants can view shared reference data. For example, MSSP users who are not administrators can view reference data that is assigned to a domain.

### Procedure

- On the navigation menu (☰), click **Admin**.
- In the **System Configuration** section, click **Reference Set Management**.
- Select the reference set that you want to add the elements to, and click **View Contents**.

4. Click the **Content** tab.
5. To add data elements manually, follow these steps:
  - a) Click **Add** and configure the parameters.

Valid port values are 0 - 65535. Valid IP addresses are between 0 and 255.255.255.255.

**Note:** If you use data obfuscation techniques on the event properties that you want to compare to the reference set data, you must use an alphanumeric reference set that contains the obfuscated data values.

- b) Click **Add**.
6. To add elements from a .csv file, follow these steps:

- a) Click **Import**.
  - b) Click **Select File** and browse to select the .csv file that you want to import.

The .csv file must be formatted with all items comma-separated on a single line, or with each item on a separate line. A delimiter is not required when each item is on a separate line.

- c) Select the **Domain** that you want to add the reference set data to.
  - d) Click **Import**.

The import adds the content of the text file to the reference set.

## Exporting elements from a reference set

Export reference set elements to a .csv file when you want to include the information in reports, or share the information with people who don't use IBM QRadar.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select the reference set that you want to export, and click **View Contents**.
4. Click the **Content** tab, and click **Export**.
5. Choose whether to open the file immediately, or save the file, and then click **OK**.

## Deleting elements from a reference set

You might need to delete elements from a reference set when an element is added to the reference set in error, or when you no longer need to compare the element with other IBM QRadar properties. For example, you might need to remove an asset that was mistakenly added to an asset exclusion blacklist.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Reference Set Management**.
3. Select the reference set that contains the elements that you want to delete, and click **View Contents**.
4. Click the **Content** tab and choose one of the following options:
  - To delete a single element, select the element from the list, and click **Delete**.
  - To delete multiple elements, use the search box to filter the list to show only the elements that you want to delete, and then click **Delete Listed**.

## Creating reference data collections with the APIs

You can use the application program interface (API) to manage IBM QRadar reference data collections.

### Procedure

1. Use a web browser to access `https://<Console IP>/api_doc` and log in as the administrator.
2. Select the latest iteration of the IBM QRadar API.
3. Select the `/reference_data` directory.
4. To create a new reference set, follow these steps:
  - a) Select `/sets`.
  - b) Click **POST** and enter the relevant information in the **Value** fields.

#### Learn more about the parameters to create a reference set:

The following table provides information about the parameters that are required to create a reference set:

| Table 19. Parameters - Reference Set |       |            |           |            |                                                  |
|--------------------------------------|-------|------------|-----------|------------|--------------------------------------------------|
| Parameter                            | Type  | Value      | Data Type | MIME Type  | Sample                                           |
| element_type                         | query | (required) | String    | text/plain | String <one of: ALN, NUM, IP, PORT, ALNIC, DATE> |
| name                                 | query | (required) | String    | text/plain | String                                           |
| fields                               | query | (optional) | String    | text/plain | field_one (field_two, field_three), field_four   |
| time_to_live                         | query | (optional) | String    | text/plain | String                                           |
| timeout_type                         | query | (optional) | String    | text/plain | String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>  |

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
5. To create a new reference map, follow these steps:
    - a) Click `/maps`.
    - b) Click **POST** and enter the relevant information in the **Value** fields.

#### Learn more about the parameters to create a reference map:

The following table provides information about the parameters that are required to create a reference map:

| Table 20. Parameters - Reference Map |       |            |           |            |                                                  |
|--------------------------------------|-------|------------|-----------|------------|--------------------------------------------------|
| Parameter                            | Type  | Value      | Data Type | MIME Type  | Sample                                           |
| element_type                         | query | (required) | String    | text/plain | String <one of: ALN, NUM, IP, PORT, ALNIC, DATE> |
| name                                 | query | (required) | String    | text/plain | String                                           |

| Table 20. Parameters - Reference Map (continued) |       |            |           |            |                                                          |
|--------------------------------------------------|-------|------------|-----------|------------|----------------------------------------------------------|
| Parameter                                        | Type  | Value      | Data Type | MIME Type  | Sample                                                   |
| fields                                           | query | (optional) | String    | text/plain | field_one<br>(field_two,<br>field_three),<br>field_four  |
| key_label                                        | query | (optional) | String    | text/plain | String                                                   |
| time_to_live                                     | query | (optional) | String    | text/plain | String                                                   |
| timeout_type                                     | query | (optional) | String    | text/plain | String <one of:<br>UNKNOWN,<br>FIRST_SEEN,<br>LAST_SEEN> |
| value_label                                      | query | (optional) | String    | text/plain | String                                                   |

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
6. To create a new reference map of sets, follow these steps:
- Select /map\_of\_sets.
  - Click **POST** and enter the relevant information in the **Value** fields.

**Learn more about the parameters to create a reference map of sets:**

The following table provides information about the parameters that are required to create a reference map of sets:

| Table 21. Parameters - Reference Map of Sets |       |            |           |            |                                                           |
|----------------------------------------------|-------|------------|-----------|------------|-----------------------------------------------------------|
| Parameter                                    | Type  | Value      | Data Type | MIME Type  | Sample                                                    |
| element_type                                 | query | (required) | String    | text/plain | String <one of:<br>ALN, NUM, IP,<br>PORT, ALNIC,<br>DATE> |
| name                                         | query | (required) | String    | text/plain | String                                                    |
| fields                                       | query | (optional) | String    | text/plain | field_one<br>(field_two,<br>field_three),<br>field_four   |
| key_label                                    | query | (optional) | String    | text/plain | String                                                    |
| time_to_live                                 | query | (optional) | String    | text/plain | String                                                    |
| timeout_type                                 | query | (optional) | String    | text/plain | String <one of:<br>UNKNOWN,<br>FIRST_SEEN,<br>LAST_SEEN>  |
| value_label                                  | query | (optional) | String    | text/plain | String                                                    |

- c) Click **Try It Out!** to finish creating the reference data collection and to view the results.
7. To create a new reference table or map of maps, follow these steps:
- Click /tables.
  - Click **POST** and enter the relevant information in the **Value** fields.

**Learn more about the parameters to create a reference table or a map of maps:**

The following table provides information about the parameters that are required to create a reference table or a map of maps:

| Table 22. Parameters - Reference Table |       |            |           |                  |                                                                                                  |
|----------------------------------------|-------|------------|-----------|------------------|--------------------------------------------------------------------------------------------------|
| Parameter                              | Type  | Value      | Data Type | MIME Type        | Sample                                                                                           |
| element_type                           | query | (required) | String    | text/plain       | String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>                                                 |
| name                                   | query | (required) | String    | text/plain       | String                                                                                           |
| fields                                 | query | (optional) | String    | text/plain       | field_one (field_two, field_three), field_four                                                   |
| key_name_types                         | query | (optional) | Array     | application/json | [ { "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>", "key_name": "String" } ] |
| outer_key_label                        | query | (optional) | String    | text/plain       | String                                                                                           |
| time_to_live                           | query | (optional) | String    | text/plain       | String                                                                                           |
| timeout_type                           | query | (optional) | String    | text/plain       | String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>                                                  |

c) Click **Try It Out!** to finish creating the reference data collection and to view the results.

### Related concepts

[Reference sets overview](#)

## Examples for using reference data collections

These examples show how you can use reference data collections to track and store data that you want to use in QRadar searches, filters, rule test conditions, and rule responses.

### Tracking expired user accounts

Use reference data collections to identify stale data, such as expired user accounts, in your IBM QRadar environment.

#### About this task

By default, reference data remains in QRadar until it is removed. However, when you create a reference data collection, you can configure QRadar to remove the data after a specified period of time.

When the data element expires, QRadar automatically deletes the value from the reference data collection and triggers an event to track the expiry.

#### Procedure

1. Create a reference set to keep track of the time since a user last logged in.

- a) Set the **Time to Live of elements** to represent the period of time after which an unused user account is considered expired.
  - b) Select the **Since last seen** button.
2. Create a custom event rule to add login data, such as the **username**, to the reference set.  
**Note:** QRadar tracks the **Date Last Seen** for each data element. If no data is added for a particular user within the time-to-live period, the reference set element expires, and a **Reference Data Expiry** event is triggered. The event contains the reference set name and the username that is expired.
  3. Use the **Log Activity** tab to track the **Reference Data Expiry** events.

### What to do next

Use the reference set data in searches, filters, rule test conditions, and rule responses.

#### Related tasks

[Adding, editing, and deleting reference sets](#)

## Integrate dynamic data from external sources

Large enterprise organizations can use reference data collections to share information about their IT assets with the security teams that manage the IBM QRadar deployment.

For example, the Information Technology (IT) team maintains an asset management database that includes information about all the network assets. Some of the information, such as the IP addresses for the web servers, changes frequently.

Once a week, the IT team exports the list of IP addresses for all of the web servers that are deployed in the network and provides the list to the security team. The security team imports the list into a reference set, which can then be used in rules, searches, and reports to provide more context to the events and flows that are processed by QRadar.



## Chapter 8. User information source configuration

Configure your IBM QRadar system to collect user and group information from Identity and Access Management endpoints.

QRadar uses the information that is collected from the endpoints to enrich the user information that is associated with the traffic and events that occur on your network.

### Related concepts

[Capabilities in your IBM QRadar product](#)

## User information source overview

You can configure a user information source to enable user information collection from an Identity and Access Management endpoint.

An Identity and Access Management endpoint is a product that collects and manages electronic user identities, group memberships, and access permissions. These endpoints are called user information sources.

Use the following utilities to configure and manage user information sources:

- **Tivoli Directory Integrator**- You must install and configure a Tivoli® Directory Integrator on a non-IBM QRadar host.
- **UISConfigUtil.sh** - Use this utility to create, retrieve, update, or delete user information sources. You can use user information sources to integrate IBM QRadar SIEM using a Tivoli Directory Integrator server.
- **GetUserInfo.sh** - Use this utility to collect user information from a user information source and store the information in a reference data collection. You can use this utility to collect user information on demand or on a schedule.

## User information sources

A user information source is a configurable component that enables communication with an endpoint to retrieve user and group information.

IBM QRadar systems support the following user information sources:

| Table 23. Supported information sources                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information Source                                                                                                                                                                           | Information that is collected                                                                                                                                                                                                                                                                                                                           |
| Microsoft Windows Active Directory (AD), version 2008 - Microsoft Windows AD is a directory service that authenticates and authorizes all users and computers that use your Windows network. | <ul style="list-style-type: none"><li>• full_name</li><li>• user_name</li><li>• user_principal_name</li><li>• family_name</li><li>• given_name</li><li>• account_is_disabled</li><li>• account_is_locked</li><li>• password_is_expired</li><li>• password_can_not_be_changed</li><li>• no_password_expired</li><li>• password_does_not_expire</li></ul> |

| Table 23. Supported information sources (continued)                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information Source                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Information that is collected                                                                                                                                 |
| IBM Security Access Manager (ISAM), version 7.0 - ISAM is an authentication and authorization solution for corporate web, client/server, and existing applications. For more information, see your IBM Security Access Manager (ISAM) documentation.                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• name_in_rgy</li> <li>• first-name</li> <li>• last-name</li> <li>• account_valid</li> <li>• password_valid</li> </ul> |
| IBM Security Identity Manager (ISIM), version 6.0 - ISIM provides the software and services to deploy policy-based provisioning solutions. This product automates the process of provisioning employees, contractors, and IBM Business Partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise. For more information, see your IBM Security Integration Manager (ISIM) documentation. | <ul style="list-style-type: none"> <li>• Full name</li> <li>• DN</li> </ul>                                                                                   |

## Reference data collections for user information

This topic provides information about how reference data collections store data collected from user information sources.

When IBM QRadar SIEM collects information from a user information source, it automatically creates a reference data collection to store the information. The name of the reference data collection is derived from the user information source group name. For example, a reference data collection that is collected from Microsoft Windows AD might be named Domain Admins.

The reference data collection type is a Map of Maps. In a Reference Map of Maps, data is stored in records that map one key to another key, which is then mapped to a single value.

For example:

- #
- # Domain Admins
- # key1,key2,data
- smith\_j,Full Name,John Smith
- smith\_j,account\_is\_disabled,0
- smith\_j,account\_is\_locked,0
- smith\_j,account\_is\_locked,1
- smith\_j,password\_does\_not\_expire,1

For more information about reference data collections, see the *Reference Data Collections Technical Note*.

## Integration workflow example

After user and group information is collected and stored in a reference data collection, there are many ways in which you can use the data in IBM QRadar SIEM.

You can create meaningful reports and alerts that characterize user adherence to your company's security policies.

Consider the following example:

To ensure activities that are performed by privileged ISIM users comply with your security policies, you can complete the following tasks:

Create a log source to collect and parse audit data for each ISIM server from which the logs are collected. For more information about how to create a log source, see the *Managing Log Sources Guide*.

1. Create a user information source for the ISIM server and collect ISIM Administrators user group information. This step creates a reference data collection that is called ISIM Administrators.
2. Configure a building block to test for events in which the source IP address is the ISIM server and the user name is listed in the ISIM administrator reference data collection. For more information about building blocks, see the *User Guide* for your product.
3. Create an event search that uses the custom building block as a filter. For more information about event searches, see the *IBM QRadar User Guide* for your product.
4. Create a custom report that uses the custom event search to generate daily reports on the audit activity of the privileged ISIM users. These generated reports indicate whether any ISIM administrator activity breaches your security policy. For more information about reports, see the *IBM QRadar User Guide* for your product.

**Note:** If you want to collect application security logs, you must create a Device Support Module (DSM). For more information, see the *IBM QRadar DSM Configuration Guide*.



## Chapter 9. IBM X-Force integration

IBM X-Force security experts use a series of international data centers to collect tens of thousands of malware samples, analyze web pages and URLs, and run analysis to categorize potentially malicious IP addresses and URLs. IBM X-Force Exchange is the platform for sharing this data, which can be used in IBM QRadar.

### Related concepts

[Capabilities in your IBM QRadar product](#)

## X-Force Threat Intelligence feed

You can integrate IBM X-Force Exchange data into IBM QRadar to help your organization stay ahead of emerging threats by identifying and remediating undesirable activity in your environment before it threatens the stability of your network.

For example, you can identify and prioritize these types of incidents:

- A series of attempted logins for a dynamic range of IP addresses
- An anonymous proxy connection to a Business Partner portal
- A connection between an internal endpoint and a known botnet command and control
- Communication between an endpoint and a known malware distribution site

**Note:** IBM X-Force integration allows you to use the X-Force Threat Intelligence data in QRadar correlation rules and AQL queries. Access to the IBM X-Force Exchange REST API is not included.

## X-Force data on the dashboard

The **Internet Threat Information Center** widget on the **Threat and Security Monitoring** dashboard uses X-Force data to provide up-to-date advisories on security issues, daily threat assessments, security news, and threat repositories.

The dashboard widget uses an embedded RSS feed to display X-Force data in the dashboard widget. The QRadar Console must have access to the internet to receive data from the X-Force update server ([www.iss.net](http://www.iss.net)).

The dashboard uses four AlertCon threat level images to provide a visual indicator of the current threat level.

| Table 24. AlertCon threat levels |                      |                                                                                                                                                    |
|----------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Level                            | Type                 | Description                                                                                                                                        |
| 1                                | Normal threats       | Ordinary activity that compromises unprotected networks, minutes to hours after QRadar connects to the internet.                                   |
| 2                                | Increased vigilance  | Vulnerabilities or online threats to computer networks that requires vulnerability assessment and corrective action.                               |
| 3                                | Focused attacks      | Specific weakness and vulnerabilities that are the target of internet attacks and require immediate defensive action.                              |
| 4                                | Catastrophic threats | Critical security situations within a network that dictate an immediate and focused defensive action. This condition might be imminent or ongoing. |

For more information about the current threat level, click the **Learn More** link to open the **Current Threat Activity** page on the IBM X-Force Exchange website.

To view a summary of the current advisories, click the arrow icon next to the advisory. To investigate the full advisory, click the advisory link.

## IBM QRadar Security Threat Monitoring Content Extension app

---

The IBM QRadar Security Threat Monitoring Content Extension app on the IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub>) contains rules, building blocks, and custom properties that are intended for use with X-Force feed data.

The X-Force data includes a list of potentially malicious IP addresses and URLs with a corresponding threat score. You use the X-Force rules to automatically flag any security event or network activity data that involves the addresses, and to prioritize the incidents before you begin to investigate them.

The following list shows examples of the types of incidents that you can identify using the X-Force rules:

- when the *[source IP/destinationIP/anyIP]* is part of any of the following *[remote network locations]*
- when *[this host property]* is categorized by X-Force as *[Anonymization Servers/Botnet C&C/DynamicIPs/Malware/ScanningIPs/Spam]* with confidence value *[equal to] [this amount]*
- when *[this URL property]* is categorized by X-Force as *[Gambling/Auctions/Job Search/Alcohol/Social Networking/Dating]*

QRadar downloads approximately 30 MB of IP reputation data per day when you enable the X-Force Threat Intelligence feed for use with the IBM QRadar Security Threat Monitoring Content Extension application.

## Installing the IBM QRadar Security Threat Monitoring Content Extension application

The IBM QRadar Security Threat Monitoring Content Extension application contains IBM QRadar content, such as rules, building blocks, and custom properties, that are designed specifically for use with X-Force data. The enhanced content can help you to identify and to remediate undesirable activity in your environment before it threatens the stability of your network.

### Before you begin

Download the IBM QRadar Security Threat Monitoring Content Extension application from the [IBM Security App Exchange](https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalThreat) (<https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalThreat>).


### About this task

To use X-Force data in QRadar rules, offenses, and events, you must configure IBM QRadar to automatically load data from the X-Force servers to your QRadar appliance.

To load X-Force data locally, enable the X-Force Threat Intelligence feed in the system settings. If new information is available when X-Force starts, the IP address reputation or URL database is updated. These updates are merged into their own databases and the content is replicated from the QRadar Console to all managed hosts in the deployment.

The X-Force rules are visible in the product even if the application is later uninstalled.

### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Extensions Management**.
3. Upload the application to the QRadar console by following these steps:
  - a) Click **Add**.
  - b) Click **Browse** to find the extension.

- c) Click **Install immediately** to install the extension without viewing the contents.
  - d) Click **Add**.
4. To view the contents of the extension, select it from the extensions list and click **More Details**.
5. To install the extension, follow these steps:
- a) Select the extension from the list and click **Install**.
  - b) If the extension does not include a digital signature, or it is signed but the signature is not associated with the IBM Security certificate authority (CA), you must confirm that you still want to install it. Click **Install** to proceed with the installation.
  - c) Review the changes that the installation makes to the system.
  - d) Select **Overwrite** or **Keep existing data** to specify how to handle existing content items.
  - e) Click **Install**.
  - f) Review the installation summary and click **OK**.

The rules appear under the **Threats** group in the **Rules List** window. They must be enabled before they are used.

## IBM X-Force Exchange plug-in for QRadar

---

IBM X-Force Exchange is a sharing platform for threat intelligence that is used by security analysts, network security specialists, and security operations center teams.

The IBM X-Force Exchange (XFE) plug-in provides the option to search the information on the IBM X-Force Exchange website for IP addresses, URLs, CVEs, and web applications that are found in QRadar. For example, you can right-click a URL from a QRadar event to see what data the X-Force Exchange contains about the URL.

You can also use the right-click lookup option to submit IP addresses or URL data from QRadar searches, offenses, and rules to a public or private collection. The collection stores the information in one place as you use the data for more research.

Collections also contain a section that serves as a wiki-style notepad, where you can add comments or any free text that is relevant. You can use the collection to save X-Force reports, text comments, or any other content. An X-Force report has both a version of the report from the time that it was saved and a link to the current version of the report.





---

## Chapter 10. Flow sources

For IBM QRadar appliances, QRadar automatically adds default flow sources for the physical ports on the appliance, and includes a default NetFlow flow source.

If QRadar is installed on your own hardware, QRadar attempts to automatically detect and add default flow sources for any physical devices, such as a network interface card (NIC). When you assign a IBM QRadar QFlow Collector, QRadar includes a default NetFlow flow source.

Flow sources are classed as either internal or external:

### Internal flow sources

Includes any additional hardware that is installed on a managed host, such as a network interface card (NIC). Depending on the hardware configuration of your managed host, the internal flow sources might include the following sources:

- Network interface card
- Napatech interface

### External flow sources

Includes any external flow sources that send flows to the QRadar QFlow Collector. If your QRadar QFlow Collector receives multiple flow sources, you can assign each flow source a distinct name. When external flow data is received by the same QRadar QFlow Collector, a distinct name helps to distinguish external flow source data from each other.

External flow sources might include the following sources:

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Flowlog file

QRadar SIEM can forward external flows source data by using the spoofing or non-spoofing method:

### Spoofing

Resends the inbound data that is received from flow sources to a secondary destination. To ensure that flow source data is sent to a secondary destination, configure the **Monitoring Interface** parameter in the flow source configuration to the port on which data is received (management port). When you use a specific interface, the QRadar QFlow Collector uses a promiscuous mode capture to obtain flow source data, rather than the default UDP listening port on port 2055. As a result, QRadar QFlow Collector can capture flow source packets and forward the data.

### Non-Spoofing

For the non-spoofing method, configure the **Monitoring Interface** parameter in the flow source configuration as Any. The QRadar QFlow Collector opens the listening port, which is the port that is configured as the **Monitoring Port** to accept flow source data. The data is processed and forwarded to another flow source destination. The source IP address of the flow source data becomes the IP address of the QRadar SIEM system, not the original router that sent the data.

## Types of flow sources

---

IBM QRadar QFlow Collector can process flows from multiple sources, which are categorized as either internal or external sources.

### Internal flow sources

Sources that include packet data by connecting to a SPAN port or a network TAP are considered internal sources. These sources provide raw packet data to a monitoring port on the Flow Collector, which converts the packet details into flow records.

QRadar does not keep the entire packet payload. Instead, it captures a snapshot of the flow, referred to as the *payload* or *content capture*, which includes packets from the beginning of the communication.

Flow collection from internal sources normally requires a dedicated Flow Collector.

### External flow sources

QRadar also supports external flow sources, such as routers that send NetFlow, sFlow, J-Flow, and Packeteer data.

External sources do not require as much CPU utilization to process so you can send them directly to a Flow Processor. In this configuration, you may have a dedicated flow collector and a flow processor, both receiving and creating flow data.

## NetFlow

NetFlow is a proprietary accounting technology that is developed by Cisco Systems. NetFlow monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a NetFlow collector.

The process of sending data from NetFlow is often referred to as a NetFlow Data Export (NDE). You can configure IBM QRadar to accept NDEs and thus become a NetFlow collector. QRadar supports NetFlow versions 1, 5, 7, and 9. For more information on NetFlow, see the [Cisco web site](http://www.cisco.com) (<http://www.cisco.com>).

While NetFlow expands the amount of the network that is monitored, NetFlow uses a connection-less protocol (UDP) to deliver NDEs. After an NDE is sent from a switch or router, the NetFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, NetFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for NetFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the IBM QRadar QFlow Collector configuration, you must also update your firewall access configuration.
- Make sure that the appropriate ports are configured for your QRadar QFlow Collector.

### Minimum recommended fields

- FIRST\_SWITCHED
- LAST\_SWITCHED
- PROTOCOL
- IPV4\_SRC\_ADDR
- IPV4\_DST\_ADDR
- L4\_SRC\_PORT
- L4\_DST\_PORT
- IN\_BYTES or OUT\_BYTES
- IN\_PKTS or OUT\_PKTS

- TCP\_FLAGS (TCP flows only)

The following VLAN fields are supported for NetFlow version 9.

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

The following fields are supported for Network Address Translation (NAT) and Network Address Port Translation (NAPT).

- postNATSourceIPv4Address
- postNATDestinationIPv4Address
- postNAPTSourceTransportPort
- postNAPTDestinationTransportPort

## IPFIX

Internet Protocol Flow Information Export (IPFIX) is an accounting technology. IPFIX monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a IPFIX collector.

IBM Security Network Protection XGS 5000, a next generation intrusion protection system (IPS), is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE). IPFIX provides more flow information and deeper insight than NetFlow v9. You can configure IBM QRadar to accept NDEs and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After an NDE is sent from the IPFIX forwarding device, the IPFIX record might be purged.

To configure QRadar to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows by using the same process.

Your QRadar system might include a default NetFlow flow source; therefore, you might not be required to configure a NetFlow flow source. To confirm that your system includes a default NetFlow flow source, on the **Admin** tab, select **Flow Sources**. If **default\_Netflow** is listed in the flow source list, IPFIX is already configured.

When you configure an external flow source for IPFIX, you must do the following tasks:

- Ensure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the IBM QRadar QFlow Collector configuration, you must also update your firewall access configuration.
- Ensure that the appropriate ports are configured for your QRadar QFlow Collector.
- Ensure that the IPFIX template from the IPFIX source includes the following IANA-listed Information Elements:
  - protocolIdentifier (4)
  - sourceIPv4Address (8)
  - destinationIPv4Address (12)
  - sourceTransportPort (7)

- destinationTransportPort (11)
- octetDeltaCount (1) or postOctetDeltaCount (23)
- packetDeltaCount (2) or postPacketDeltaCount (24)
- tcpControlBits (6) (TCP flows only)
- flowStartSeconds (150) or flowStartMilliseconds (152) or flowStartDeltaMicroseconds (158)
- flowEndSeconds (151) or flowEndMilliseconds (153) or flowEndDeltaMicroseconds (159)

The following VLAN fields are supported for IPFIX.

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

The following MPLS fields are supported for IPFIX.

- mplsTopLabelType
- mplsTopLabelIPv4Address
- mplsTopLabelStackSection
- mplsLabelStackSection2
- mplsLabelStackSection3
- mplsLabelStackSection4
- mplsLabelStackSection5
- mplsLabelStackSection6
- mplsLabelStackSection7
- mplsLabelStackSection8
- mplsLabelStackSection9
- mplsLabelStackSection10
- mplsVpnRouteDistinguisher
- mplsTopLabelPrefixLength
- mplsTopLabelIPv6Address
- mplsPayloadLength
- mplsTopLabelTTL
- mplsLabelStackLength
- mplsLabelStackDepth
- mplsTopLabelExp
- postMplsTopLabelExp
- pseudoWireType
- pseudoWireControlWord
- mplsLabelStackSection
- mplsPayloadPacketSection

- sectionOffset
- sectionExportedOctets

For more information about these MPLS fields, see [IP Flow Information Export \(IPFIX\) Entities \(https://www.iana.org/assignments/ipfix/ipfix.xhtml\)](https://www.iana.org/assignments/ipfix/ipfix.xhtml).

## sFlow

sFlow is a multi-vendor and user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously.

A sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. IBM QRadar supports sFlow versions 2, 4, and 5. sFlow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information, see the [sFlow website \(www.sflow.org\)](http://www.sflow.org).

sFlow uses a connection-less protocol (UDP). When data is sent from a switch or router, the sFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, sFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

When you configure an external flow source for sFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that the appropriate ports are configured for your QRadar VFlow Collector.

## J-Flow

A proprietary accounting technology used by Juniper Networks that allows you to collect IP traffic flow statistics. J-Flow enables you to export data to a UDP port on a J-Flow collector. Using J-Flow, you can also enable J-Flow on a router or interface to collect network statistics for specific locations on your network.

Note that J-Flow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information on J-Flow, see the [Juniper Networks website \(www.juniper.net\)](http://www.juniper.net).

J-Flow uses a connection-less protocol (UDP). When data is sent from a switch or router, the J-Flow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, J-Flow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for J-Flow, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure the appropriate ports are configured for your IBM QRadar QFlow Collector.

The following VLAN fields are supported for J-Flow.

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

## Packeteer

Packeteer devices collect, aggregate, and store network performance data. After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to IBM QRadar.

Packeteer uses a connection-less protocol (UDP). When data is sent from a switch or router, the Packeteer record is purged. As UDP is used to send this information and does not guarantee the delivery of data, Packeteer records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might occur.

To configure Packeteer as an external flow source, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.
- Make sure that you configure Packeteer devices to export flow detail records and configure the IBM QRadar QFlow Collector as the destination for the data export.
- Make sure that the appropriate ports are configured for your QRadar QFlow Collector.
- Make sure the class IDs from the Packeteer devices can automatically be detected by the QRadar QFlow Collector.
- For more information, see the *Mapping Packeteer Applications into QRadar Technical Note*.

## Flowlog file

A Flowlog file is generated from the IBM QRadar flow logs.

## Napatech interface

If you installed a Napatech Network Adapter on your IBM QRadar system, the **Napatech Interface** option is displayed as a configurable packet-based flow source on the QRadar user interface. The Napatech Network Adapter provides next-generation programmable and intelligent network adapter for your network. For more information, see the Napatech documentation.

## Adding or editing a flow source

---

Use the **Flow Source** window to add a flow source.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Do one of the following actions:
  - To add a flow source, click **Add**.
  - To edit a flow source, select the flow source and click **Edit**.
4. To create this flow source from an existing flow source, select the **Build from existing flow source** check box, and select a flow source from the **Use as Template** list.
5. Enter the name for the **Flow Source Name**.

**Tip:** If the external flow source is also a physical device, use the device name as the flow source name. If the flow source is not a physical device, use a recognizable name.

For example, if you want to use IPFIX traffic, enter **ipf1**. If you want to use NetFlow traffic, enter **nf1**.
6. Select a flow source from the **Flow Source Type** list and configure the properties.
  - If you select the **Flowlog File** option, ensure that you configure the location of the Flowlog file for the **Source File Path** parameter.
  - If you select the **JFlow**, **Netflow**, **Packeteer FDR**, or **sFlow** options in the **Flow Source Type** parameter, ensure that you configure an available port for the **Monitoring Port** parameter.

The default port for the first NetFlow flow source that is configured in your network is 2055. For each additional NetFlow flow source, the default port number increments by 1. For example, the default NetFlow flow source for the second NetFlow flow source is 2056.

- If you select the **Napatech Interface** option, enter the **Flow Interface** that you want to assign to the flow source.

**Restriction:** The **Napatech Interface** option is displayed only if you installed the Napatech Network Adapter on your system.

- If you select the **Network Interface** option, for the **Flow Interface**, configure only one log source for each Ethernet interface.

**Restriction:** You cannot send different flow types to the same port.

7. If traffic on your network is configured to take alternate paths for inbound and outbound traffic, select the **Enable Asymmetric Flows** check box.
8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.

## Enabling and disabling a flow source

---

Using the **Flow Source** window, you can enable or disable a flow source.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Select the flow source that you want to enable or disable, and click **Enable/Disable**.
4. On the **Admin** tab, click **Deploy Changes**.

## Deleting a Flow Source

---

Use the **Flow Source** window to delete a flow source.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Select the flow source that you want to delete, and click **Delete**.
4. On the **Admin** tab, click **Deploy Changes**.

## Flow source aliases

---

A flow source alias uses a virtual name to identify external flows that are sent to the same port on a flow collector. For example, the IBM QRadar QFlow Collector can have a single NetFlow flow source that is listening on port 2055, and can have multiple NetFlow sources sending to the same QRadar QFlow Collector. By using flow source aliases, you can identify the different NetFlow sources based by their IP addresses.

When QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, the QRadar QFlow Collector attempts a reverse DNS lookup. The lookup is used to determine the host name of the device.

You can configure the QRadar QFlow Collector to automatically create flow source aliases. When the QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, it does a reverse DNS lookup to determine the host name of the device.

If the lookup is successful, the QRadar QFlow Collector adds this information to the database and reports the information to all QRadar QFlow Collector components in your deployment. If the lookup fails, QRadar creates a default alias for the flow source based on the flow source name and the source IP address. For example, the default alias might appear as **default\_NetFlow\_172.16.10.139**.

## Adding a flow source alias

Use the **Flow Source Alias** window to add a flow source alias.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Source Aliases**.
3. Do one of the following actions:
  - To add a flow source alias, click **Add** and enter the values for the parameters.
  - To edit an existing flow source alias, select the flow source alias, click **Edit**, and update the parameters.
4. Click **Save**.
5. On the **Admin** tab, click **Deploy Changes**.

**Note:** If you rename a flow source alias, you must use the original name to perform a historical search.

## Deleting a flow source alias

Use the **Flow Source Alias** window to delete a flow source alias.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Source Aliases**.
3. Select the flow source alias that you want to delete, and then click **Delete**.
4. On the **Admin** tab menu, click **Deploy Changes**.

## Correcting flow time stamps

You can specify the way that you want flow time stamps to be handled when Netflow V9 begins sending records with overflowed system uptime values.

### About this task

Two new configuration settings provide more control over the way that flow time stamps are handled when Netflow V9 begins sending records with overflowed system uptime values. The new settings eliminate the need to reset the first and last switched times.

The new configuration options and the default values are shown here:

- NORMALISE\_OVERFLOWED\_UPTIMES=YES
- UPTIME\_OVERFLOW\_THRESHOLD\_MSEC=86400000

The time stamps are corrected when the system uptime value is less than the first and last switched packet times by more than the value that is specified in the UPTIME\_OVERFLOW\_THRESHOLD\_MSEC configuration. The time stamps are corrected based on the assumption that the system uptime wrapped around the maximum 32-bit value.



## Procedure

1. To change these settings, add the settings to the `/store/configservices/staging/globalconfig/nva.conf` file.
2. To fine-tune the settings, specify a different time interval for the `UPTIME_OVERFLOW_THRESHOLD_MSEC` setting.
3. To disable this feature, set the `NORMALISE_OVERFLOWED_UPTIMES` to `NO`.

When this feature is disabled, QRadar does not modify the NetFlow v9 time stamps that meet this condition.

4. After you change the configuration settings, you must deploy the system.



# Chapter 11. Remote networks and services configuration

Use remote network and service groups to represent traffic activity on your network for a specific profile. Remote networks groups display user traffic that originates from named remote networks.

All remote network and service groups have group levels and leaf object levels. You can edit remote network and service groups by adding objects to existing groups or changing preexisting properties to suit your environment.

If you move an existing object to another group, the object name moves from the existing group to the newly selected group. However, when the configuration changes are deployed, the object data that is stored in the database is lost and the object ceases to function. To resolve this issue, create a new view and re-create the object that exists with another group.

You can group remote networks and services for use in the custom rules engine, flow, and event searches. You can also group networks and services in IBM QRadar Risk Manager, if it is available.

## Related concepts

[Capabilities in your IBM QRadar product](#)

## Default remote network groups

IBM QRadar includes default remote network groups.

The following table describes the default remote network groups.

| Table 25. Default remote network groups |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
| BOT                                     | <p>Specifies traffic that originates from BOT applications.</p> <p>For more information, see <a href="http://rules.emergingthreats.net/blockrules/emerging-botcc.rules">Botnet Command and Control drop rules on the Emerging Threats website</a> (<a href="http://rules.emergingthreats.net/blockrules/emerging-botcc.rules">http://rules.emergingthreats.net/blockrules/emerging-botcc.rules</a>)</p>          |
| Bogon                                   | <p>Specifies traffic that originates from unassigned IP addresses.</p> <p>For more information, see <a href="http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt">bogon reference on the Team CYMRU website</a> (<a href="http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt">http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt</a>).</p>                                       |
| HostileNets                             | <p>Specifies traffic that originates from known hostile networks.</p> <p>HostileNets has a set of 20 (rank 1 - 20 inclusive) configurable CIDR ranges.</p> <p>For more information, see <a href="http://www.dshield.org/ipsascii.html?limit=20">HostileNets reference on the DShield website</a> (<a href="http://www.dshield.org/ipsascii.html?limit=20">http://www.dshield.org/ipsascii.html?limit=20</a>)</p> |

| Table 25. Default remote network groups (continued) |                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group                                               | Description                                                                                                                                                                                                                                                                     |
| Neighbours                                          | Specifies traffic that originates from nearby networks that your organization has network peering agreements with.<br><br>This group is blank by default. You must configure this group to classify traffic that originates from neighboring networks.                          |
| Smurfs                                              | Specifies traffic that originates from smurf attacks.<br><br>A smurf attack is a type of denial-of-service attack that floods a destination system with spoofed broadcast ping messages.                                                                                        |
| Superflows                                          | This group is non-configurable.<br><br>A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.                                                                                                                       |
| TrustedNetworks                                     | Specifies traffic from trusted networks, including business partners that have remote access to your critical applications and services.<br><br>This group is blank by default.<br><br>You must configure this group to classify traffic that originates from trusted networks. |
| Watchlists                                          | Classifies traffic that originates from networks that you want to monitor.<br><br>This group is blank by default.                                                                                                                                                               |

Groups and objects that include superflows are only for informational purposes and cannot be edited. Groups and objects that include bogons are configured by the automatic update function.

**Note:** You can use reference sets instead of remote networks to provide some of this functionality. Although you can assign a confidence level to an IP value in a reference table, reference sets are used only with single IPs and cannot be used with CIDR ranges. You can use a CIDR value after a remote network update, but not with weight or confidence levels.

#### Related concepts

“Types of reference data collections” on page 69

IBM QRadar has different types of reference data collections that can handle different levels of data complexity. The most common types are reference sets and reference maps.

## Default remote service groups

IBM QRadar includes the default remote service groups.

The following table describes the default remote service groups.

Table 26. Default remote network groups

| Parameter          | Description                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------|
| IRC_Servers        | Specifies traffic that originates from addresses commonly known as chat servers.                              |
| Online_Services    | Specifies traffic that originates from addresses commonly known online services that might involve data loss. |
| Porn               | Specifies traffic that originates from addresses commonly known to contain explicit pornographic material.    |
| Proxies            | Specifies traffic that originates from commonly known open proxy servers.                                     |
| Reserved_IP_Ranges | Specifies traffic that originates from reserved IP address ranges.                                            |
| Spam               | Specifies traffic that originates from addresses commonly known to produce SPAM or unwanted email.            |
| Spy_Adware         | Specifies traffic that originates from addresses commonly known to contain spyware or adware.                 |
| Superflows         | Specifies traffic that originates from addresses commonly known to produce superflows.                        |
| Warez              | Specifies traffic that originates from addresses commonly known to contain pirated software.                  |

## Guidelines for network resources

Given the complexities and network resources that are required for IBM QRadar SIEM in large structured networks, follow the suggested guidelines.

The following list describes some of the suggested practices that you can follow:

- Bundle objects and use the **Network Activity** and **Log Activity** tabs to analyze your network data.  
Fewer objects create less input and output to your disk.
- Typically, for standard system requirements, do not exceed more than 200 objects per group.  
More objects might impact your processing power when you investigate your traffic.



## Managing remote networks objects

After you create remote network groups, you can aggregate flow and event search results on remote network groups. You can also create rules that test for activity on remote network groups.

Use the **Remote Networks** window, you can add or edit a remote networks object.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Remote Networks and Services Configuration** section, click **Remote Networks and Services**.
3. To add a remote networks object, click **Add** and enter values for the parameters.
4. To edit a remote networks object, follow these steps:
  - a) Double-click the group name.

- b) Select the profile and click the edit icon (  ) to edit the remote profile.
5. Click **Save**.
6. Click the previous icon (  ) to go back to the **Remote Networks and Services** window .
7. On the **Admin** tab, click **Deploy Changes**.


## Managing remote services objects

---

Remote services groups organize traffic that originates from user-defined network ranges or the IBM automatic update server. After you create remote service groups, you can aggregate flow and event search results, and create rules that test for activity on remote service groups.

Use the **Remote Services** window to add or edit a remote services object.

### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **Remote Networks and Services Configuration** section, click **Remote Networks and Services**.
3. To add a remote services object, click **Add** and enter the parameter values.
4. To edit a remote services object, click the group that you want displayed, click the **Edit** icon and change the values.
5. Click **Save**.
6. Click **Return**.
7. Close the **Remote Services** window.
8. On the **Admin** tab menu, click **Deploy Changes**.

---

## Chapter 12. Server discovery

The **Server Discovery** function uses the Asset Profile database to discover different server types that are based on port definitions. Then, you can select the servers to add to a server-type building block for rules.

The **Server Discovery** function is based on server-type building blocks. Ports are used to define the server type. Thus, the server-type building block works as a port-based filter when you search the Asset Profile database.

For more information about building blocks, see the *IBM QRadar User Guide*.

Use the **Server Discovery** function with IBM QRadar Vulnerability Manager to create exception rules for benign vulnerabilities. Reduce the number of vulnerabilities that you see for the following **Server Types**:

| Table 27. Server type vulnerabilities |                        |
|---------------------------------------|------------------------|
| Server Type                           | Vulnerability          |
| FTP Servers                           | FTP Server Present     |
| DNS Servers                           | DNS Server is Running  |
| Mail Servers                          | SMTP Server Detected   |
| Web Servers                           | Web Service is Running |

For more information about false positive vulnerabilities, see the *IBM QRadar Vulnerability Manager User Guide*.

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## Discovering servers

Use the **Assets** tab to discover servers on your network.

### Procedure

1. On the navigation menu (☰), click **Assets** to open the **Assets** tab.
2. On the **Assets** navigation menu, click **Server Discovery**.
3. From the **Server Type** list, select the server type that you want to discover.
4. Select one of the following options to determine the servers you want to discover:
  - To use the currently selected **Server Type** to search all servers in your deployment, select **All**.
  - To search servers in your deployment that were assigned to the currently selected **Server Type**, select **Assigned**.
  - To search servers in your deployment that are not assigned, select **Unassigned**.
5. To edit the standard server port list, click **Edit ports**.
6. From the **Network** list, select the network that you want to search.
7. Click **Discover Servers**.
8. In the **Matching Servers** table, select the check boxes of all servers you want to assign to the server role.
9. Click **Approve Selected Servers**.





---

## Chapter 13. Domain segmentation

Segmenting your network into different domains helps to ensure that relevant information is available only to those users that need it.

You can create security profiles to limit the information that is available to a group of users within that domain. Security profiles provide authorized users access to only the information that is required to complete their daily tasks. You modify only the security profile of the affected users, and not each user individually.

You can also use domains to manage overlapping IP address ranges. This method is helpful when you are using a shared IBM QRadar infrastructure to collect data from multiple networks. By creating domains that represent a particular address space on the network, multiple devices that are in separate domains can have the same IP address and still be treated as separate devices.

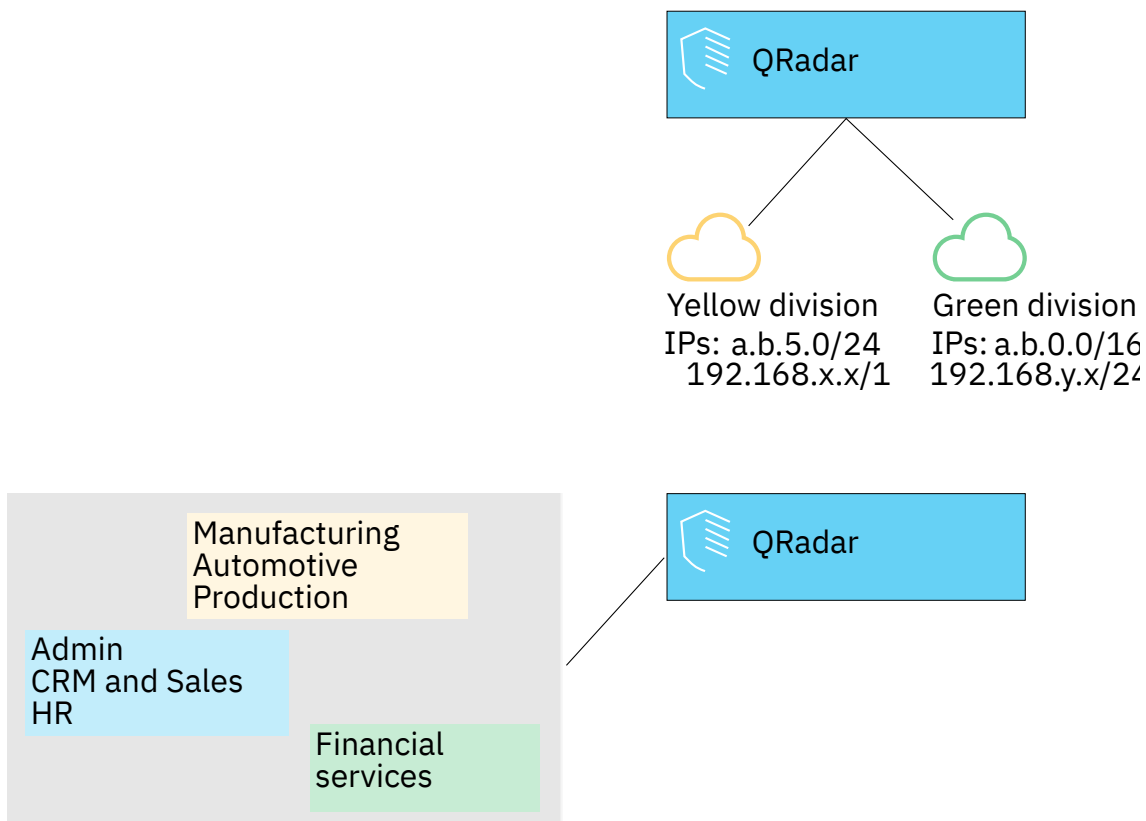


Figure 10. Domain segmentation

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## Overlapping IP addresses

An overlapping IP address is an IP address that is assigned to more than one device or logical unit, such as an event source type, on a network. Overlapping IP address ranges can cause significant problems for companies that merge networks after corporate acquisitions, or for Managed Security Service Providers (MSSPs) who are bringing on new clients.

IBM QRadar must be able to differentiate events and flows that come from different devices and that have the same IP address. If the same IP address is assigned to more than one event source, you can create domains to distinguish them.

For example, let's look at a situation where Company A acquires Company B and wants to use a shared instance of QRadar to monitor the new company's assets. The acquisition has a similar network structure that results in the same IP address being used for different log sources in each company. Log sources that have the same IP address cause problems with correlation, reporting, searching, and asset profiling.

To distinguish the origin of the events and flows that come in to QRadar from the log source, you can create two domains and assign each log source to a different domain. If required, you can also assign each event collector, flow collector, or data gateway to the same domain as the log source that sends events to them.

To view the incoming events by domain, create a search and include the domain information in the search results.

## Domain definition and tagging

Domains are defined based on IBM QRadar input sources. When events and flows come into QRadar, the domain definitions are evaluated and the events and flows are tagged with the domain information.

### Specifying domains for events

The following diagram shows the precedence order for evaluating domain criteria for events.

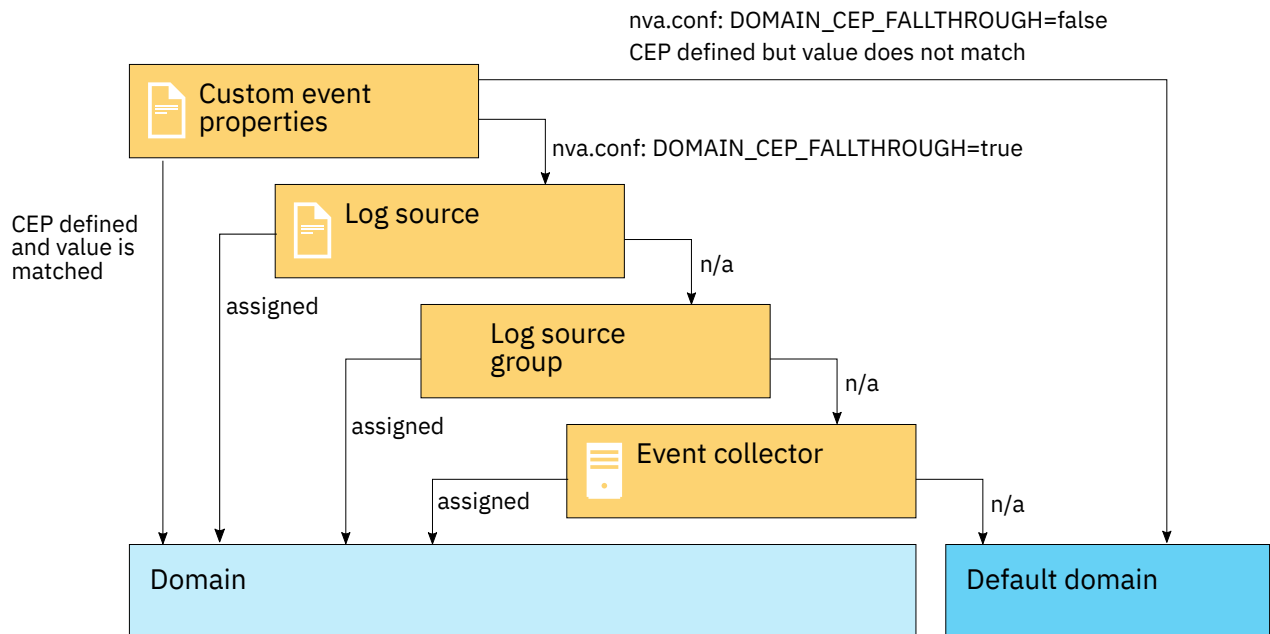


Figure 11. Precedence order for events

These are the ways to specify domains for events:

#### Event collectors and data gateways

If an event collector or data gateway is dedicated to a specific network segment or IP address range, you can flag that entire event collector or data gateway as part of that domain.

All log sources that arrive at that event collector or data gateway belong to the domain; therefore, any new auto-detected log sources are automatically added to the domain.

#### Important:

If an event source is redirected from one event collector or data gateway to another in a different domain, you must update its log source in one of the following ways:

- Edit the log source to update the event collector or data gateway information.
- Delete the log source and deploy the full configuration so that the event source is auto-detected on the new event collector or data gateway.

Unless the log source is updated, non-admin users with domain restrictions might not see offenses that are associated with the log source.

### Log sources

You can configure specific log sources to belong to a domain.

This method of tagging domains is an option for deployments in which an event collector or data gateway can receive events from multiple domains.

### Log source groups

You can assign log source groups to a specific domain. This option allows broader control over the log source configuration.

Any new log sources that are added to the log source group automatically get the domain tagging that is associated with the log source group.

### Custom properties

You can apply custom properties to the log messages that come from a log source.

To determine which domain that specific log messages belong to, the value of the custom property is looked up against a mapping that is defined in the Domain Management editor.

This option is used for multi-address-range or multi-tenant log sources, such as file servers and document repositories.

## Specifying domains for flows

The following diagram shows the precedence order for evaluating domain criteria for flows.

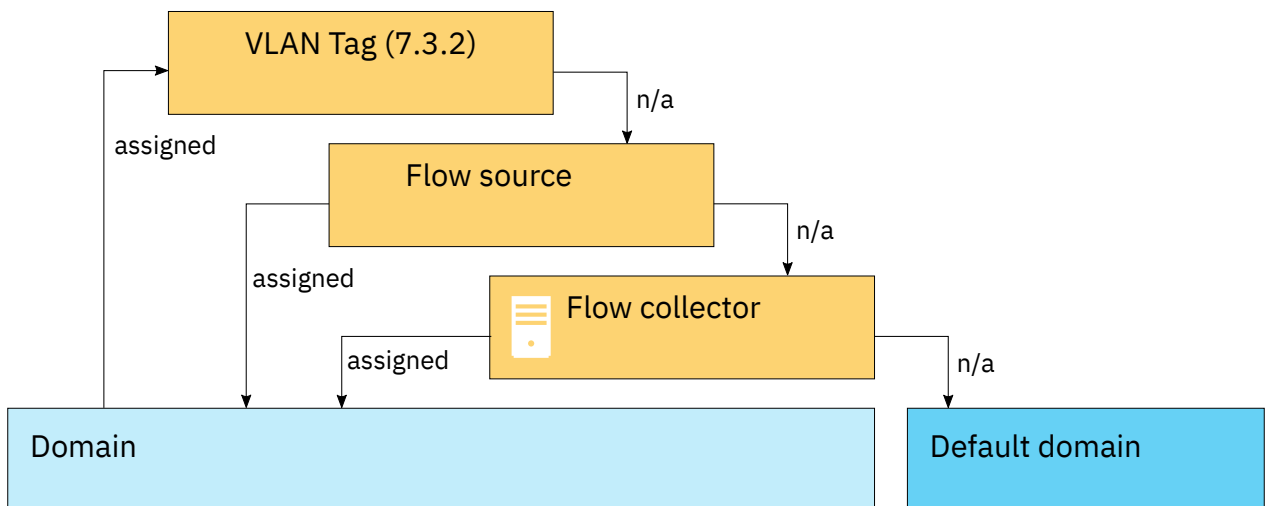


Figure 12. Precedence order for flows

These are the ways to specify domains for flows:

### Flow collectors and data gateways

You can assign specific data gateways to a domain.

All flow sources that arrive at that flow collector or data gateway belong to the domain; therefore, any new auto-detected flow sources are automatically added to the domain.

### Flow sources

You can designate specific flow sources to a domain.

This option is useful when a single flow collector or data gateway is collecting flows from multiple network segments or routers that contain overlapping IP address ranges.

### **Flow VLAN ID**

You can designate specific VLANs to a domain.

This option is useful when you collect traffic from multiple network segments, often with overlapping IP ranges. This VLAN definition is based on the Enterprise and Customer VLAN IDs.

The following information elements are sent from QFlow when flows that contain VLAN information are analyzed. These two fields can be assigned in a domain definition:

- PEN 2 (IBM), element ID 82: Enterprise VLAN ID
- PEN 2 (IBM), element ID 83: Customer VLAN ID

## **Specifying domains for scan results**

You can also assign vulnerability scanners to a specific domain so that scan results are properly flagged as belonging to that domain. A domain definition can consist of all QRadar input sources.

For more information about assigning your network to preconfigured domains, see [“Network hierarchy” on page 25](#).

## **Precedence order for evaluating domain criteria**

When events and flows come into the QRadar system, the domain criteria is evaluated based on the granularity of the domain definition.

If the domain definition is based on an event, the incoming event is first checked for any custom properties that are mapped to the domain definition. If the result of a regular expression that is defined in a custom property does not match a domain mapping, the event is automatically assigned to the default domain.

If the event does not match the domain definition for custom properties, the following order of precedence is applied:

1. Log source
2. Log source group
3. Event collector or data gateway

If the domain is defined based on a flow, the following order of precedence is applied:

1. Flow source
2. Flow collector or data gateway

If a scanner has an associated domain, all assets that are discovered by the scanner are automatically assigned to the same domain as the scanner.

## **Forwarding data to another QRadar system**

Domain information is removed when data is forwarded to another QRadar system. Events and flows that contain domain information are automatically assigned to the default domain on the receiving QRadar system. To identify which events and flows are assigned to the default domain, you can create a custom search on the receiving system. You might want to reassign these events and flows to a user-defined domain.

## Creating domains

---

Use the **Domain Management** window to create domains based on IBM QRadar input sources.


### About this task

Use the following guidelines when you create domains:

- Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. Users who have limited domain access should not have administrative privileges because this privilege grants unlimited access to all domains.
- You can map the same custom property to two different domains, however the capture result must be different for each one.
- You cannot assign a log source, log source group, event collector, or data gateway to two different domains. When a log source group is assigned to a domain, each of the mapped attributes is visible in the **Domain Management** window.

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes deployed.

### Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **System Configuration** section, click **Domain Management**.
3. To add a domain, click **Add** and type a unique name and description for the domain.  
**Tip:** You can check for unique names by typing the name in the **Input domain name** search box.
4. Depending on the domain criteria to be defined, click the appropriate tab.
  - To define the domain based on a custom property, log source group, log source, event collector, or data gateway, click the **Events** tab.
  - To define the domain based on a flow source, click the **Flows** tab.
  - To define the domain based on a scanner, including IBM QRadar Vulnerability Manager scanners, click the **Scanners** tab.
5. To assign a custom property to a domain, in the **Capture Result** box, type the text that matches the result of the regular expression (regex) filter.  
**Important:** You must select the **Optimize parsing for rules, reports, and searches** check box in the **Custom Event Properties** window to parse and store the custom event property. Domain segmentation will not occur if this option is not checked.
6. From the list, select the domain criteria and click **Add**.
7. After you add the source items to the domain, click **Create**.

### What to do next

Create security profiles to define which users have access to the domains. After you create the first domain in your environment, you must update the security profiles for all non-administrative users to specify the domain assignment. In domain-aware environments, non-administrative users whose security profile does not specify a domain assignment will not see any log activity or network activity.

Review the hierarchy configuration for your network, and assign existing IP addresses to the proper domains. For more information, see [“Network hierarchy” on page 25](#).

## Creating domains for VLAN flows

Use the **Domain Management** window to create domains based on IBM QRadar VLAN flow sources.

### About this task

In QRadar, you can assign domains to incoming flows based on the VLAN information that is contained in the flow. The incoming flows are mapped to domains that contain the same VLAN definition.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Domain Management**.
3. Click **Add** and type a unique name and description for the domain.

**Tip:** You can check for unique names by typing the name in the **Input domain name** search box.

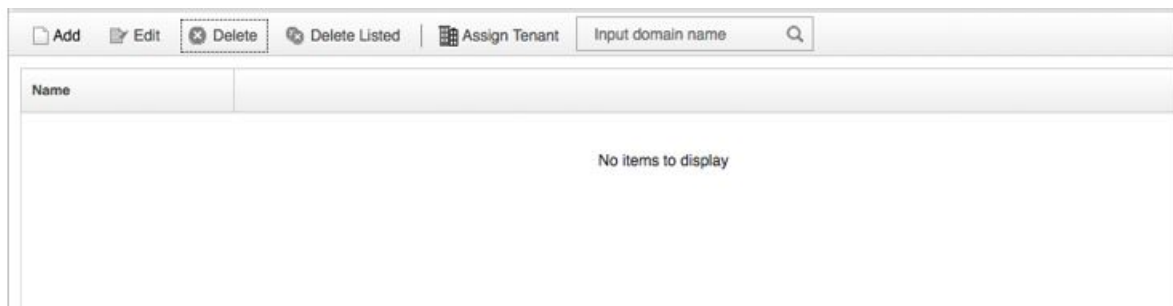


Figure 13. Input domain name

4. Click the **Flows** tab, and then select **Flow VLAN IDs**.
5. Select the enterprise VLAN ID and Customer VLAN ID values that match the values on the incoming flows, and then click **Add**.

#### Notes:

- The Enterprise VLAN ID (IE): 82 is specified by Private Enterprise Number (PEN): 2, Information Element (IE) on incoming flows.
- The Customer VLAN ID is specified by PEN: 2 and IE: 83 on incoming flows.

Figure 14. New Domain

6. In the **Name** field, type a unique name for the domain and then click **Create**.

## Results

The domain definition is created and incoming flows are mapped. Tenant assignment to a domain occurs as normal.

| Name          | Flow VLAN IDs                   |
|---------------|---------------------------------|
| ExampleDomain | Enterprise: 500 ; Customer: 100 |

Figure 15. Domain definition created

## Domain privileges that are derived from security profiles

You can use security profiles to grant domain privileges and ensure that domain restrictions are respected throughout the entire IBM QRadar system. Security profiles also make it easier to manage privileges for a large group of users when your business requirements suddenly change.

Users can see only data within the domain boundaries that are set up for the security profiles that are assigned to them. Security profiles include domains as one of the first criteria that is evaluated to restrict access to the system. When a domain is assigned to a security profile, it takes priority over other security permissions. After domain restrictions are evaluated, individual security profiles are assessed to determine network and log permissions for that particular profile.

For example, a user is given privileges to Domain\_2 and access to network 10.0.0.0/8. That user can see only events, offenses, assets, and flows that come from Domain\_2 and contain an address from the 10.0.0.0/8 network.

As a QRadar administrator, you can see all domains and you can assign domains to non-administrative users. Do not assign administrative privileges to users whom you want to limit to a particular domain.

Security profiles must be updated with an associated domain. Domain-level restrictions are not applied until the security profiles are updated, and the changes are deployed.

When you assign domains to a security profile, you can grant access to the following types of domains:

#### **User-defined domains**

You can create domains that are based on input sources by using the Domain Management tool. For more information, see [Creating domains](#).

#### **Default domain**

Everything that is not assigned to a user-defined domain is automatically assigned to the default domain. The default domain contains system-wide events.

**Note:** Users who have access to the default domain can see system-wide events without restriction. Ensure that this access is acceptable before you assign default domain access to users. All administrators have access to the default domain.

Any log source that gets auto-discovered on a shared event collector or data gateway (one that is not explicitly assigned to a domain), is auto-discovered on the default domain. These log sources require manual intervention. To identify these log sources, you must periodically run a search in the default domain that is grouped by log source.

#### **All domains**

Users who are assigned to a security profile that has access to **All Domains** can see all active domains within the system, the default domain, and any domains that were previously deleted across the entire system. They can also see all domains that are created in the future.

If you delete a domain, it cannot be assigned to a security profile. If the user has the **All domains** assignment, or if the domain was assigned to the user before it was deleted, the deleted domain is returned in historical search results for events, flows, assets, and offenses. You can't filter by deleted domains when you run a search.

Administrative users can see which domains are assigned to the security profiles on the **Summary** tab in the **Domain Management** window.

### **Rule modifications in domain-aware environments**

Rules can be viewed, modified, or disabled by any user who has both the **Maintain Custom Rules** and **View Custom Rules** permissions, regardless of which domain that user belongs to.

**Important:** When you add the **Log Activity** capability to a user role, the **Maintain Custom Rules** and **View Custom Rules** permissions are automatically granted. Users who have these permissions have access to all log data for all domains, and they can edit rules in all domains, even if their security profile settings have domain-level restrictions. To prevent domain users from being able to access log data and modify rules in other domains, edit the user role and remove the **Maintain Custom Rules** and **View Custom Rules** permissions.

### **Domain-aware searches**

You can use domains as search criteria in custom searches. Your security profile controls which domains you can search against.

System-wide events and events that are not assigned to a user-defined domain are automatically assigned to the default domain. Administrators, or users who have a security profile that provides access to the default domain, can create a custom search to see all events that are not assigned to a user-defined domain.

The default domain administrator can share a saved search with other domain users. When the domain user runs that saved search, the results are limited to their domain.



## Domain-specific rules and offenses

A rule can work in the context of a single domain or in the context of all domains. Domain-aware rules provide the option of including the **And Domain Is** test.

The following diagram shows an example using multiple domains.

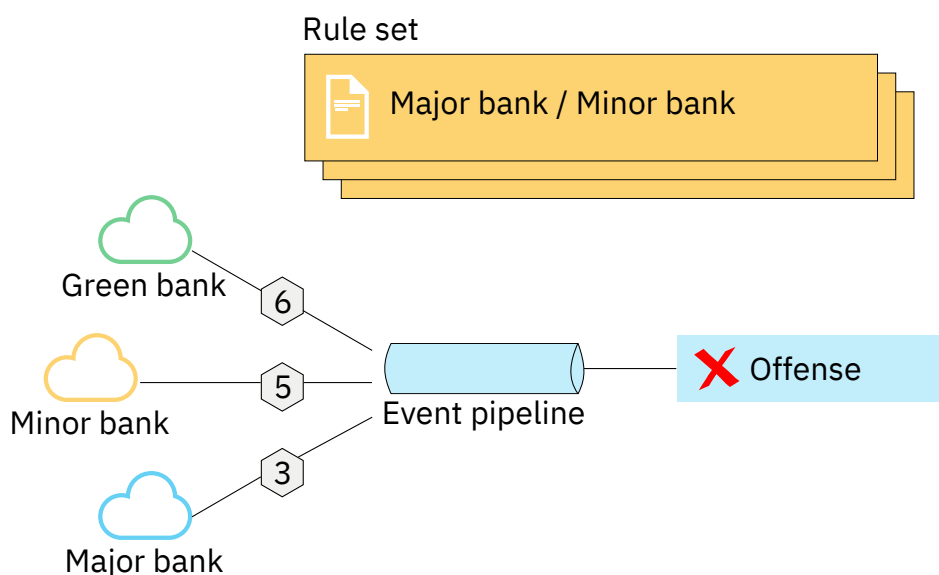


Figure 16. Domain aware rules

You can restrict a rule so that it is applied only to events that are happening within a specified domain. An event that has a domain tag that is different from the domain that is set on the rule does not trigger an event response.

In an IBM QRadar system that does not have user-defined domains, a rule creates an offense and keeps contributing to it each time the rule fires. In a domain-aware environment, a rule creates a new offense each time the rule is triggered in the context of a different domain.

Rules that work in the context of all domains are referred to as system-wide rules. To create a system-wide rule that tests conditions across the entire system, select **Any Domain** in the domain list for the **And Domain Is** test. An **Any Domain** rule creates an **Any Domain** offense.

### Single-domain rule

If the rule is a stateful rule, the states are maintained separately for each domain. The rule is triggered separately for each domain. When the rule is triggered, offenses are created separately for each domain that is involved and the offenses are tagged with those domains.

### Single-domain offense

The offense is tagged with the corresponding domain name. It can contain only events that are tagged with that domain.

### System-wide rule

If the rule is a stateful rule, a single state is maintained for the whole system and domain tags are ignored. When the rule runs, it creates or contributes to a single system-wide offense.

### System-wide offense

The offense is tagged with **Any Domain**. It contains only events that are tagged with all domains.

The following table provides examples of domain-aware rules. The examples use a system that has three domains that are defined: Domain\_A, Domain\_B, and Domain\_C.

The rule examples in the following table may not be applicable in your QRadar environment. For example, rules that use flows and offenses are not applicable in IBM QRadar Log Manager.

Table 28. Domain-aware rules

| Domain text                                                                                                                                   | Explanation                                                                                                                                                                                                                                                                        | Rule response                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain is one of: Domain_A</b>                                                                                                             | Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.                                                                                                                                                                           | Creates or contributes to an offense that is tagged with Domain_A.                                                                                                                                                                                                                                                       |
| <b>domain is one of: Domain_A</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b>           | Looks only at events that are tagged with Domain_A and ignores rules that are tagged with other domains.                                                                                                                                                                           | Creates or contributes to an offense that is tagged with Domain_A. A single state, an HTTP flow counter, gets maintained for Domain_A.                                                                                                                                                                                   |
| <b>domain is one of: Domain_A, Domain_B</b>                                                                                                   | Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C.<br><br>This rule behaves as two independent instances of a single domain rule, and creates separate offenses for different domains.                              | For data that is tagged with Domain_A, it creates or contributes to a single domain offense that is tagged with Domain_A.<br><br>For data that is tagged with Domain_B, it creates or contributes to a single domain offense that is tagged with Domain_B.                                                               |
| <b>domain is one of: Domain_A, Domain_B</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> | Looks only at events that are tagged with Domain_A and Domain_B and ignores events that are tagged with Domain_C.<br><br>This rule behaves as two independent instances of a single domain rule, and maintains two separate states (HTTP flow counters) for two different domains. | When the rule detects 10 HTTP flows that are tagged with Domain_A within a minute, it creates or contributes to an offense that is tagged with Domain_A.<br><br>When the rule detects 10 HTTP flows that are tagged with Domain_B within a minute, it creates or contributes to an offense that is tagged with Domain_B. |
| No domain test defined                                                                                                                        | Looks at events that are tagged with all domains and creates or contributes to offenses on a per-domain basis.                                                                                                                                                                     | Each independent domain has offenses that are generated for it, but offenses do not contain contributions from other domains.                                                                                                                                                                                            |
| A rule has a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> and no domain test is defined        | Looks at events that are tagged with Domain_A, Domain_B, or Domain_C.                                                                                                                                                                                                              | Maintains separate states and creates separate offenses for each domain.                                                                                                                                                                                                                                                 |
| <b>domain is one of: Any Domain</b>                                                                                                           | Looks at all events, regardless of which domain it is tagged with.                                                                                                                                                                                                                 | Creates or contributes to a single system-wide offense that is tagged with Any Domain.                                                                                                                                                                                                                                   |

Table 28. Domain-aware rules (continued)

| Domain text                                                                                                                           | Explanation                                                                                                         | Rule response                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domain is one of: Any Domain</b> and a stateful test that is defined as <b>when HTTP flow is detected 10 times within 1 minute</b> | Looks at all events, regardless of which domain it is tagged with, and it maintains a single state for all domains. | Creates or contributes to a single system-wide offense that is tagged with Any Domain.<br><br>For example, if it detects 3 events that are tagged with Domain_A, 3 events that are tagged with Domain_B, and 4 events that are tagged with Domain_C within 1 minute, it creates an offense because it detected 10 events in total. |
| <b>domain is one of: Any Domain, Domain_A</b>                                                                                         | Works the same as a rule that has <b>domain is one of: Any Domain</b> .                                             | When the domain test includes Any Domain, any single domains that are listed are ignored.                                                                                                                                                                                                                                          |

When you view the offense table, you can sort the offenses by clicking the **Domain** column. The **Default Domain** is not included in the sort function so it does not appear in alphabetical order. However, it appears at the top or bottom of the **Domain** list, depending on whether the column is sorted in ascending or descending order. **Any Domain** does not appear in the list of offenses.

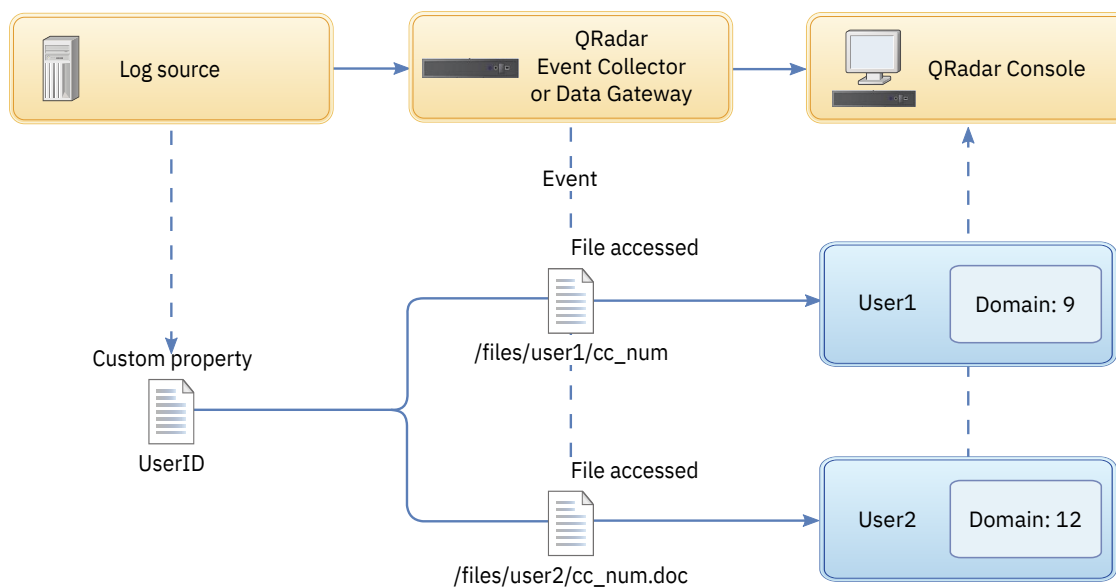
## Example: Domain privilege assignments based on custom properties

If your log files contain information that you want to use in a domain definition, you can expose the information as a custom event property.

You assign a custom property to a domain based on the capture result. You can assign the same custom property to multiple domains, but the capture results must be different.

For example, a custom event property, such as `userID`, might evaluate to a single user or a list of users. Each user can belong to only one domain.

In the following diagram, the log sources contain user identification information that is exposed as a custom property, `userID`. The event collector or data gateway returns two user files, and each user is assigned to only one domain. In this case, one user is assigned to Domain: 9 and the other user is assigned to Domain: 12.



*Figure 17. Assigning domains by using custom event property*

If the capture results return a user that is not assigned to a specific user-defined domain, that user is automatically assigned to the default domain. Default domain assignments require manual intervention. Perform periodic searches to ensure that all entities in the default domain are correctly assigned.

**Important:** Before you use a custom property in a domain definition, ensure that **Optimize parsing for rules, reports, and searches** is checked on the **Custom Event Properties** window. This option ensures that the custom event property is parsed and stored when IBM QRadar receives the event for the first time. Domain segmentation doesn't occur if this option is not checked.

---

## Chapter 14. Multitenant management

Multitenant environments allow Managed Security Service Providers (MSSPs) and multi-divisional organizations to provide security services to multiple client organizations from a single, shared IBM QRadar deployment. You don't have to deploy a unique QRadar instance for each customer.

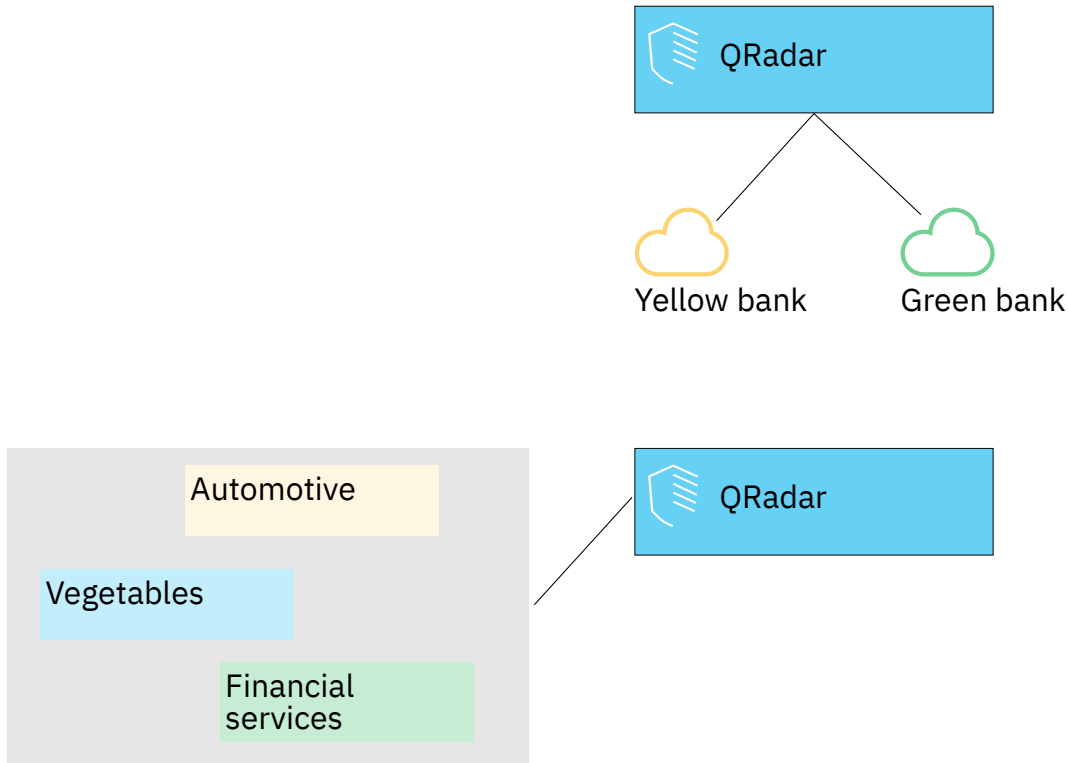


Figure 18. Multitenant environments

In a multitenant deployment, you ensure that customers see only their data by creating domains that are based on their QRadar input sources. Then, use security profiles and user roles to manage privileges for large groups of users within the domain. Security profiles and user roles ensure that users have access to only the information that they are authorized to see.

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## User roles in a multitenant environment

Multitenant environments include a service provider and multiple tenants. Each role has distinct responsibilities and associated activities.

### Service provider

The service provider owns the system and manages its use by multiple tenants. The service provider can see data across all tenants. The Managed Security Service Provider (MSSP) administrator is typically responsible for the following activities:

- Administers and monitors the system health of the IBM QRadar deployment.
- Provisions new tenants.
- Creates roles and security profiles for tenant administrators and users.
- Secures the system against unauthorized access.

- Creates domains to isolate tenant data.
- Deploys changes that the tenant administrator made in the tenant environment.
- Monitors QRadar licenses.
- Collaborates with the tenant administrator.

## Tenants

Each tenancy includes a tenant administrator and tenant users. The tenant administrator can be an employee of the tenant organization, or the service provider can administer the tenant on behalf of the customer.

The tenant administrator is responsible for the following activities:

- Configures network hierarchy definitions within their own tenancy.
- Configures and manages tenant data.
- Views log sources. Can edit the log source to coalesce data and can disable log sources.
- Collaborates with the MSSP administrator.

The tenant administrator can configure tenant-specific deployments, but they can't access or change the configuration for another tenant. They must contact the MSSP administrator to deploy changes in the QRadar environment, including network hierarchy changes within their own tenant.

Tenant users have no administrative privileges and can see only the data that they have access to. For example, a user can have privileges to view data from only 1 log source within a domain that has multiple log sources.

## Domains and log sources in multitenant environments

---

Use domains to separate overlapping IP addresses, and to assign sources of data, such as events and flows, into tenant-specific data sets.

When events or flows come into IBM QRadar, QRadar evaluates the domain definitions that are configured, and the events and flows are assigned to a domain. A tenant can have more than one domain. If no domains are configured, the events and flows are assigned to the default domain.

### Domain segmentation

Domains are virtual buckets that you use to segregate data based on the source of the data. They are the building blocks for multitenant environments. You configure domains from the following input sources:

- Event and flow collectors
- Flow sources
- Log sources and log source groups
- Custom properties
- Scanners

A multitenant deployment might consist of a basic hardware configuration that includes one QRadar Console, one centralized event processor, and then one event collector for each customer. In this configuration, you define domains at the collector level, which then automatically assigns the data that is received by QRadar to a domain.

To consolidate the hardware configuration even further, you can use one collector for multiple customers. If log or flow sources are aggregated by the same collector but belong to different tenants, you can assign the sources to different domains. When you use domain definitions at the log source level, each log source name must be unique across the entire QRadar deployment.

If you need to separate data from a single log source and assign it to different domains, you can configure domains from custom properties. QRadar looks for the custom property in the payload, and assigns it to

the correct domain. For example, if you configured QRadar to integrate with a Check Point Provider-1 device, you can use custom properties to assign the data from that log source to different domains.

## Automatic log source detection

When domains are defined at the collector level and the dedicated event collector is assigned to a single domain, new log sources that are automatically detected are assigned to that domain. For example, all log sources that are detected on `Event_Collector_1` are assigned to `Domain_A`. All log sources that are automatically collected on `Event_Collector_2` are assigned to `Domain_B`.

When domains are defined at the log source or custom property level, log sources that are automatically detected and are not already assigned to a domain are automatically assigned to the default domain. The MSSP administrator must review the log sources in the default domain and allocate them to the correct client domains. In a multitenant environment, assigning log sources to a specific domain prevents data leakage and enforces data separation across domains.

## Provisioning a new tenant

---

As a Managed Security Services Provider (MSSP) administrator, you are using a single instance of IBM QRadar to provide multiple customers with a unified architecture for threat detection and prioritization.

In this scenario, you are onboarding a new client. You provision a new tenant and create a tenant administrator account that does limited administrative duties within their own tenant. You limit the access of the tenant administrator so that they can't see or edit information in other tenants.

Before you provision a new tenant, you must create the data sources, such as log sources or flow collectors, for the customer and assign them to a domain.

Complete the following tasks by using the tools on the **Admin** tab to provision the new tenant in QRadar:

1. To create the tenant, click **Tenant Management**.

For information about setting events per second (EPS) and flows per minute (FPM) limits for each tenant, see [“Monitoring license usage in multitenant deployments” on page 117](#).

2. To assign domains to the tenant, click **Domain Management**.
3. To create the tenant administrator role and grant the **Delegated Administration** permissions, click **User Roles**.

In a multitenant environment, tenant users with **Delegated administration** permissions can see only data for their own tenant environment. If you assign other administrative permissions that are not part of **Delegated Administration**, access is no longer restricted to that domain.

4. To create the tenant security profiles and restrict data access by specifying the tenant domains, click **Security Profiles**.
5. To create the tenant users and assign the user role, security profile, and tenant, click **Users**.

## Monitoring license usage in multitenant deployments

---

As the Managed Security Service Provider (MSSP) administrator, you monitor the event and flow rates across the entire IBM QRadar deployment.

When you create a tenant, you can set limits for both events per second (EPS) and flows per minute (FPM). By setting EPS and FPM limits for each tenant, you can better manage license capacities across multiple clients. If you have a processor that is collecting events or flows for a single customer, you do not need to assign tenant EPS and FPM limits. If you have a single processor that collects events or flows for multiple customers, you can set EPS and FPM limits for each tenant.

If you set the EPS and FPM limits to values that exceed the limits of either your software licenses or the appliance hardware, the system automatically throttles the events and flows for that tenant to ensure that the limits are not exceeded. If you do not set EPS and FPM limits for tenants, each tenant receives events and flows until either the license limits or the appliance limits are reached. The licensing limits are applied

to the managed host. If you regularly exceed the license limitations, you can get a different license that is more suitable for your deployment.

## Viewing EPS rates per log source

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rates for log sources.

1. On the **Log Activity** tab, select **Advanced Search** from the list on the **Search** toolbar.
2. To view the EPS per log source, type the following AQL query in the **Advanced Search** field:

```
select logsourceName(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by logsourceid
order by EPS desc
last 24 hours
```

## Viewing EPS rates per domain

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) query to view the EPS rates for domains.

1. On the **Log Activity** tab, select **Advanced Search** from the drop-down list box on the **Search** toolbar.
2. To view the EPS per domain, type the following AQL query in the **Advanced Search** field:

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by domainid
order by EPS desc
last 24 hours
```

If you want to view average EPS rates for log sources only, click **Log Sources** in the **Data Sources** pane on the **Admin** tab. You can use this to quickly identify configuration issues with log sources that are failing to report.

## Rules management in multitenant deployments

In a multitenant environment, you must customize rules to make them tenant-aware. Tenant-aware rules use the **when the domain is one of the following** rule test, but the domain modifier determines the scope of the rule.

The following table shows how you can use the domain modifier to change the scope of rules in a multitenant deployment.

| Table 29. Scope of rules in a multitenant environment |                                                                                                                                                                  |                                                                                          |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Rule scope                                            | Description                                                                                                                                                      | Rule test example                                                                        |
| Single domain rules                                   | These rules include only 1 domain modifier.                                                                                                                      | <b>and when the domain is one of the following:</b> <i>manufacturing</i>                 |
| Single tenant rules                                   | These rules include all the domains that are assigned to the tenant. Use single tenant rules to correlate events across multiple domains within a single tenant. | <b>and when the domain is one of the following:</b> <i>manufacturing, finance, legal</i> |
| Global rules                                          | These rules use the <b>Any domain</b> modifier and run across all tenants.                                                                                       | <b>and when the domain is one of the following:</b> <i>Any domain</i>                    |

By being domain-aware, the custom rules engine (CRE) automatically isolates event correlations from different tenants by using their respective domains. For more information about working with rules in a domain-segmented network, see [Chapter 13, “Domain segmentation,”](#) on page 103.



## Network hierarchy updates in a multitenant deployment

---

IBM QRadar uses the network hierarchy to understand and analyze the network traffic in your environment. Tenant administrators who have the **Define network hierarchy** permission can change the network hierarchy within their own tenant.

Network hierarchy changes require a full configuration deployment to apply the updates in the QRadar environment. Full configuration deployments restart all QRadar services, and data collection for events and flows stops until the deployment completes. Tenant administrators must contact the Managed Security Service Provider (MSSP) administrator to deploy the changes. MSSP administrators can plan the deployment during a scheduled outage, and notify all tenant administrators in advance.

In a multitenant environment, the network object name must be unique across the entire deployment. You cannot use network objects that have the same name, even if they are assigned to different domains.

### **Related concepts**

#### Network hierarchy

IBM QRadar uses the network hierarchy objects and groups to view network activity and monitor groups or services in your network.



---

## Chapter 15. Asset Management

Assets and asset profiles that are created for servers and hosts in your network provide important information to assist you in resolving security issues. Using the asset data, you can connect offenses that are triggered in your system to physical or virtual assets to provide a starting point in a security investigation.

The **Assets** tab in IBM QRadar provides a unified view of the known information about the assets in your network. As QRadar discovers more information, the system updates the asset profile and incrementally builds a complete picture about the asset.

Asset profiles are built dynamically from identity information that is passively absorbed from event or flow data, or from data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually. For more information, see the topics *Importing Asset Profiles* and *Adding or editing an asset profile* in the *IBM QRadar User Guide*.

**Restriction:** IBM QRadar Log Manager tracks only asset data if IBM QRadar Vulnerability Manager is installed. For more information about the differences between QRadar SIEM and QRadar Log Manager, see [“Capabilities in your IBM QRadar product”](#) on page 7.

### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## Sources of asset data

Asset data is received from several different sources in your IBM QRadar deployment.

Asset data is written to the asset database incrementally, usually 2 or 3 pieces of data at a time. With exception of updates from network vulnerability scanners, each asset update contains information about only one asset at a time.

Asset data usually comes from one of the following asset data sources:

### Events

Event payloads, such as those created by DHCP or authentication servers, often contain user logins, IP addresses, host names, MAC addresses, and other asset information. This data is immediately provided to the asset database to help determine which asset the asset update applies to.

Events are the primary cause for asset growth deviations.

### Flows

Flow payloads contain communication information such as IP address, port, and protocol that is collected over regular, configurable intervals. At the end of each interval, the data is provided to the asset database, one IP address at a time.

Because asset data from flows is paired with an asset based on a single identifier, the IP address, flow data is never the cause of asset growth deviations.

### Vulnerability scanners

QRadar integrates with both IBM and third-party vulnerability scanners that can provide asset data such as operating system, installed software, and patch information. The type of data varies from scanner to scanner and can vary from scan to scan. As new assets, port information, and vulnerabilities are discovered, data is brought into the asset profile based on the CIDR ranges that are defined in the scan.

It is possible for scanners to introduce asset growth deviations but it is rare.

### User interface

Users who have the Assets role can import or provide asset information directly to the asset database. Asset updates that are provided directly by a user are for a specific asset. Therefore the asset reconciliation stage is bypassed.

Asset updates that are provided by users do not introduce asset growth deviations.

## **Domain-aware asset data**

When an asset data source is configured with domain information, all asset data that comes from that data source is automatically tagged with the same domain. Because the data in the asset model is domain-aware, the domain information is applied to all QRadar components, including identities, offenses, asset profiles, and server discovery.

When you view the asset profile, some fields might be blank. Blank fields exist when the system did not receive this information in an asset update, or the information exceeded the asset retention period. The default retention period is 120 days. An IP address that appears as 0.0.0.0 indicates that the asset does not contain IP address information.

## Incoming asset data workflow

---

IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

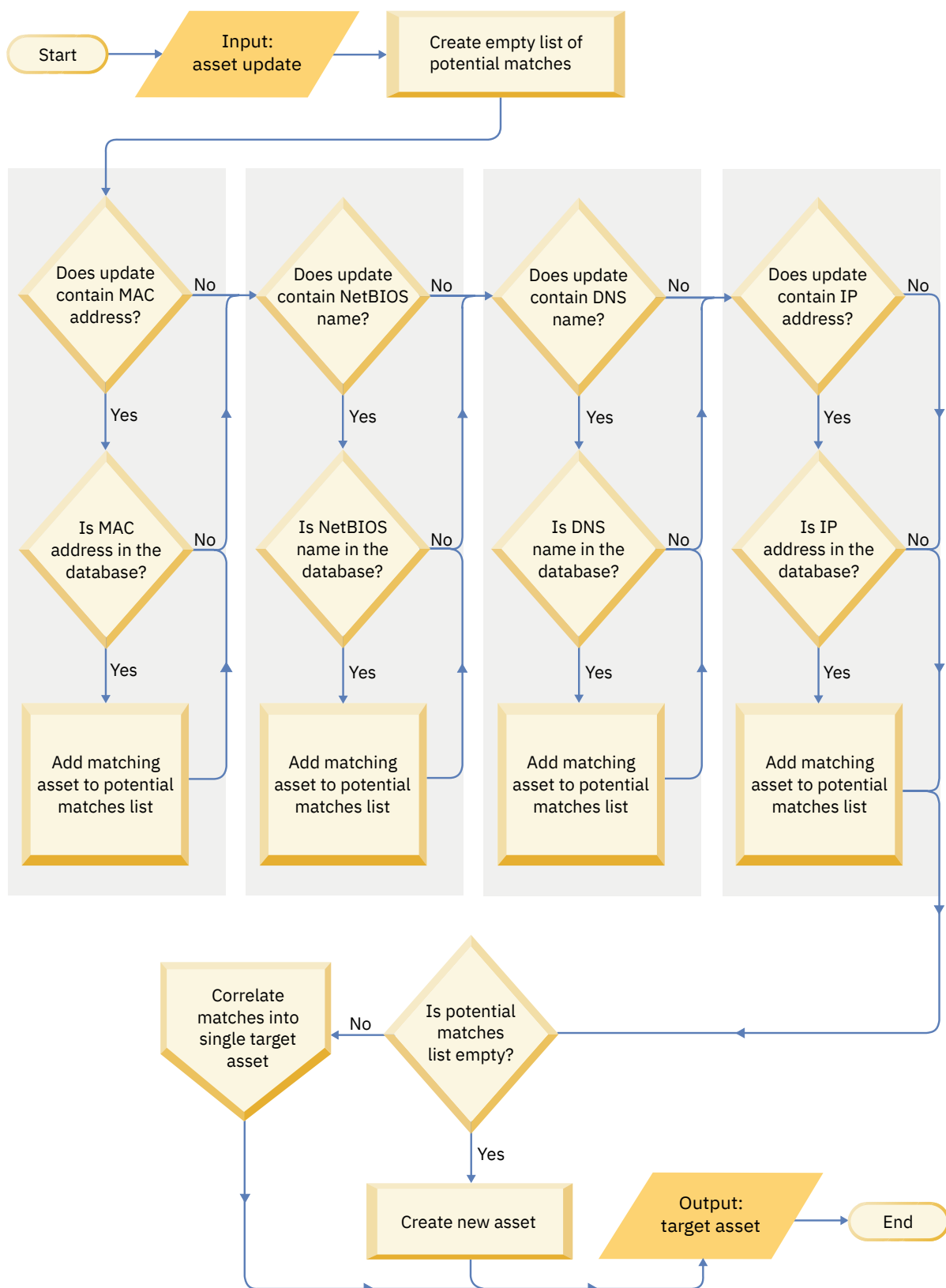


Figure 19. Asset data workflow diagram

1. QRadar receives the event. The asset profiler examines the event payload for identity information.

2. If the identity information includes a MAC address, a NetBIOS host name, or a DNS host name that are already associated with an asset in the asset database, then that asset is updated with any new information.
3. If the only available identity information is an IP address, the system reconciles the update to the existing asset that has the same IP address.
4. If an asset update has an IP address that matches an existing asset but the other identity information does not match, the system uses other information to rule out a false-positive match before the existing asset is updated.
5. If the identity information does not match an existing asset in the database, then a new asset is created based on the information in the event payload.

## Updates to asset data

---

IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Each asset update must contain trusted information about a single asset. When QRadar receives an asset update, the system determines which asset to which the update applies.

*Asset reconciliation* is the process of determining the relationship between asset updates and the related asset in the asset database. Asset reconciliation occurs after QRadar receives the update but before the information is written to the asset database.

### Identity information

Every asset must contain at least one piece of identity data. Subsequent updates that contain one or more pieces of that same identity data are reconciled with the asset that owns that data. Updates that are based on IP addresses are handled carefully to avoid false-positive asset matches. False positive asset matches occur when one physical asset is assigned ownership of an IP address that was previously owned by another asset in the system.

When multiple pieces of identity data are provided, the asset profiler prioritizes the information from the most deterministic to the least in the following order:

- MAC address
- NetBIOS host name
- DNS host name
- IP address

MAC addresses, NetBIOS host names, and DNS host names are unique and therefore are considered as definitive identity data. Incoming updates that match an existing asset only by the IP address are handled differently than updates that match more definitive identity data.

### Asset reconciliation exclusion rules

With each asset update that enters IBM QRadar, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

By default, each piece of asset data is tracked over a two-hour period. If any one piece of identity data in the asset update exhibits suspicious behavior two or more times within 2 hours, that piece of data is added to the asset blacklists. Each type of identity asset data that is tested results in a new blacklist.

**Tip:** QRadar excludes events based on data that is received in the event, not on any data that is later inferred or linked to the event.

In domain-aware environments, the asset reconciliation exclusion rules track the behavior of asset data separately for each domain.

The asset reconciliation exclusion rules test the following scenarios:

| Table 30. Rule tests and responses                                                                  |                                                                                |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Scenario                                                                                            | Rule response                                                                  |
| When a MAC address is associated to three or more different IP addresses in 2 hours or less         | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |
| When a DNS host name is associated to three or more different IP addresses in 2 hours or less       | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less   | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less      | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less  | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When a DNS host name is associated to three or more different MAC addresses in 2 hours or less      | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When an IPv4 address is associated to three or more different DNS host names in 2 hours or less     | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less | Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist |
| When a MAC address is associated to three or more different DNS host names in 2 hours or less       | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |
| When an IPv4 address is associated to three or more different NetBIOS host names in 2 hours or less | Add the IP address to the Asset Reconciliation Domain IPv4 blacklist           |
| When a DNS host name is associated to three or more different NetBIOS host names in 2 hours or less | Add the DNS host name to the Asset Reconciliation Domain DNS blacklist         |
| When a MAC address is associated to three or more different NetBIOS host names in 2 hours or less   | Add the MAC address to the Asset Reconciliation Domain MAC blacklist           |

You can view these rules on the **Offenses** tab by clicking **Rules** and then selecting the **asset reconciliation exclusion** group in the drop-down list.

## Asset merging

*Asset merging* is the process where the information for one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Asset merging occurs when an asset update contains identity data that matches two different asset profiles. For example, a single update that contains a NetBIOS host name that matches one asset profile and a MAC address that matches a different asset profile might trigger an asset merge.

Some systems can cause high volumes of asset merging because they have asset data sources that inadvertently combine identity information from two different physical assets into a single asset update. Some examples of these systems include the following environments:

- Central syslog servers that act as an event proxy
- Virtual machines
- Automated installation environments
- Non-unique host names, common with assets like iPads and iPhones.



- Virtual private networks that have shared MAC addresses
- Log source extensions where the identity field is `OverrideAndAlwaysSend=true`

Assets that have many IP addresses, MAC addresses, or host names show deviations in asset growth and can trigger system notifications.

## Identification of asset growth deviations

Sometimes, asset data sources produce updates that IBM QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

*Asset growth deviations* occur when the number of asset updates for a single device grows beyond the limit that is set by the retention threshold for a specific type of the identity information. Proper handling of asset growth deviations is critical to maintaining an accurate asset model.

At the root of every asset growth deviation is an asset data source whose data is untrustworthy for updating the asset model. When a potential asset growth deviation is identified, you must look at the source of the information to determine whether there is a reasonable explanation for the asset to accumulate large amounts of identity data. The cause of an asset growth deviation is specific to an environment.

### DHCP server example of unnatural asset growth in an asset profile

Consider a virtual private network (VPN) server in a Dynamic Host Configuration Protocol (DHCP) network. The VPN server is configured to assign IP addresses to incoming VPN clients by proxying DHCP requests on behalf of the client to the network's DHCP server.

From the perspective of the DHCP server, the same MAC address repeatedly requests many IP address assignments. In the context of network operations, the VPN server is delegating the IP addresses to the clients, but the DHCP server can't distinguish when a request is made by one asset on behalf of another.

The DHCP server log, which is configured as a QRadar log source, generates a DHCP acknowledgment (DHCP ACK) event that associates the MAC address of the VPN server with the IP address that it assigned to the VPN client. When asset reconciliation occurs, the system reconciles this event by MAC address, which results in a single existing asset that grows by one IP address for every DHCP ACK event that is parsed.

Eventually, one asset profile contains every IP address that was allocated to the VPN server. This asset growth deviation is caused by asset updates that contain information about more than one asset.

### Threshold settings

When an asset in the database reaches a specific number of properties, such as multiple IP addresses or MAC addresses, QRadar blocks that asset from receiving more updates.

The Asset Profiler threshold settings specify the conditions under which an asset is blocked from updates. The asset is updated normally up to the threshold value. When the system collects enough data to exceed the threshold, the asset shows an asset growth deviation. Future updates to the asset are blocked until the growth deviation is rectified.

## System notifications that indicate asset growth deviations

IBM QRadar generates system notifications to help you identify and manage the asset growth deviations in your environment.

The following system messages indicate that QRadar identified potential asset growth deviations:

- The system detected asset profiles that exceed the normal size threshold
- The asset blacklist rules have added new asset data to the asset blacklists

The system notification messages include links to reports to help you identify the assets that have growth deviations.

### Asset data that changes frequently

Asset growth can be caused by large volumes of asset data that changes legitimately, such as in these situations:

- A mobile device that travels from office-to-office frequently and is assigned a new IP address whenever it logs in.
- A device that connects to a public wifi with short IP addresses leases, such as at a university campus, might collect large volumes of asset data over a semester.

## Example: How configuration errors for log source extensions can cause asset growth deviations

Customized log source extensions that are improperly configured can cause asset growth deviations.

You configure a customized log source extension to provide asset updates to IBM QRadar by parsing user names from the event payload that is on a central log server. You configure the log source extension to override the event host name property so that the asset updates that are generated by the custom log source always specify the DNS host name of the central log server.

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

## Troubleshooting asset profiles that exceed the normal size threshold

IBM QRadar generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

```
The system detected asset profiles that exceed the normal size threshold
```

### Explanation

The payload of the notification shows a list of the top five most frequently deviating assets and why the system marked each asset as a growth deviation. As shown in the following example, the payload also shows the number of times that the asset attempted to grow beyond the asset size threshold.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

When the asset data exceeds the configured threshold, QRadar blocks the asset from future updates. This intervention prevents the system from receiving more corrupted data and mitigates the performance impacts that might occur if the system attempts to reconcile incoming updates against an abnormally large asset profile.

### Required user action

Use the information in the notification payload to identify the assets that are contributing to the asset growth deviation and determine what is causing the abnormal growth. The notification provides a link to a report of all assets that experienced deviating asset growth over the past 24 hours.

After you resolve the asset growth deviation in your environment, you can run the report again.

1. Click the **Log Activity** tab and click **Search > New Search**.
2. Select the **Deviating Asset Growth: Asset Report** saved search.
3. Use the report to identify and repair inaccurate asset data that was created during the deviation.

### Related concepts

#### Stale asset data

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.

## New asset data is added to the asset blacklists

IBM QRadar generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

```
The asset blacklist rules have added new asset data to the asset blacklists
```

### Explanation

Asset exclusion rules monitor asset data for consistency and integrity. The rules track specific pieces of asset data over time to ensure that they are consistently being observed with the same subset of data within a reasonable time.

For example, if an asset update includes both a MAC address and a DNS host name, the MAC address is associated with that DNS host name for a sustained period. Subsequent asset updates that contain that MAC address also contain that same DNS host name when one is included in the asset update. If the MAC address suddenly is associated with a different DNS host name for a short period, the change is monitored. If the MAC address changes again within a short period, the MAC address is flagged as contributing to an instance of deviating or abnormal asset growth.

### Required user action

Use the information in the notification payload to identify the rules that are used to monitor asset data. Click the **Asset deviations by log source** link in the notification to see the asset deviations that occurred in the last 24 hours.

If the asset data is valid, QRadar administrators can configure QRadar to resolve the problem.

- If your blacklists are populating too aggressively, you can tune the asset reconciliation exclusion rules that populate them.
- If you want to add the data to the asset database, you can remove the asset data from the blacklist and add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.

### Related concepts

#### Advanced tuning of asset reconciliation exclusion rules

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

## Prevention of asset growth deviations

After you confirm that the reported asset growth is legitimate, there are several ways to prevent IBM QRadar from triggering growth deviation messages for that asset.

Use the following list to help you decide how to prevent asset growth deviations:

- Understand how QRadar handles stale asset data.
- Create identity exclusion searches to exclude certain events from providing asset updates.

- [Tune the Asset Reconciliation Exclusion rules](#) to refine the definition of deviating asset growth.
- Create asset whitelists to prevent data from reappearing on the asset blacklists.
- Modify the entries on the asset blacklists and asset whitelists.
- Ensure that your DSMs are up to date. QRadar provides a weekly automatic update that might contain DSM updates and corrections to parsing issues.

## Stale asset data

Stale asset data can be problematic when the rate at which new asset records are created exceeds the rate at which stale asset data is removed. Controlling and managing asset retention thresholds is the key to addressing asset growth deviations that are caused by stale asset data.

*Stale asset data* is historical asset data that is not actively or passively observed within a specific time. Stale asset data is deleted when it exceeds the configured retention period.

The historical records become active again if they are observed by IBM QRadar passively, through events and flows, or actively, through port and vulnerability scanners.

Preventing asset growth deviations requires finding the right balance between the number of IP addresses allowed for a single asset and the length of time that QRadar retains the asset data. You must consider the performance and manageability trade-offs before you configure QRadar to accommodate high levels of asset data retention. While longer retention periods and higher per-asset thresholds might appear desirable all the time, a better approach is to determine a baseline configuration that is acceptable for your environment and test that configuration. Then, you can increase the retention thresholds in small increments until the right balance is achieved.

## Asset blacklists and whitelists

IBM QRadar uses a group of asset reconciliation rules to determine if asset data is trustworthy. When asset data is questionable, QRadar uses asset blacklists and whitelists to determine whether to update the asset profiles with the asset data.

An *asset blacklist* is a collection of data that QRadar considers untrustworthy. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

The asset blacklists and whitelists are reference sets. You can view and modify the asset blacklist and whitelist data using the **Reference Set Management** tool in the QRadar Console. For more information about working with reference sets, see [“Reference sets overview”](#) on page 70.

### Asset blacklists

An *asset blacklist* is a collection of data that IBM QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

Every asset update in QRadar is compared to the asset blacklists. Blacklisted asset data is applied globally for all domains. If the asset update contains identity information (MAC address, NetBIOS host name, DNS host name, or IP address) that is found on a blacklist, the incoming update is discarded and the asset database is not updated.

The following table shows the reference collection name and type for each type of identity asset data.

Table 31. Reference collection names for asset blacklist data

| Type of identity data                                                                       | Reference collection name              | Reference collection type        |
|---------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|
| IP addresses (v4)                                                                           | Asset Reconciliation IPv4 Blacklist    | Reference Set [Set Type: IP]     |
| DNS host names                                                                              | Asset Reconciliation DNS Blacklist     | Reference Set [Set Type: ALNIC*] |
| NetBIOS host names                                                                          | Asset Reconciliation NetBIOS Blacklist | Reference Set [Set Type: ALNIC*] |
| MAC Addresses                                                                               | Asset Reconciliation MAC Blacklist     | Reference Set [Set Type: ALNIC*] |
| * ALNIC is an alphanumeric type that can accommodate both host name and MAC address values. |                                        |                                  |

You can use the **Reference Set Management** tool to edit the blacklist entries. For information about working with reference sets, see [Reference sets management](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html) ([http://www.ibm.com/support/knowledgecenter/SS42VS\\_7.2.7/com.ibm.qradar.doc/c\\_qradar\\_adm\\_mge\\_ref\\_set.html](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html)).

## Related concepts

[Asset whitelists](#)

## Asset whitelists

You can use asset whitelists to keep IBM QRadar asset data from inadvertently reappearing in the asset blacklists.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

You can use the **Reference Set Management** tool to edit the whitelist entries. For information about working with reference sets, see [Reference sets management](#).

## Example of a whitelist use case

The whitelist is helpful if you have asset data that continues to show up in the blacklists when it is a valid asset update. For example, you might have a round robin DNS load balancer that is configured to rotate across a set of five IP addresses. The Asset Reconciliation Exclusion rules might determine that the multiple IP addresses associated with the same DNS host name are indicative of an asset growth deviation, and the system might add the DNS load balancer to the blacklist. To resolve this problem, you can add the DNS host name to the Asset Reconciliation DNS Whitelist.

## Mass entries to the asset whitelist

An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network. Ignoring asset deviations by adding mass entries to the asset whitelist is not helpful in building an accurate asset database. Instead of adding mass whitelist entries, review the asset blacklist to determine what is contributing to the deviating asset growth and then determine how to fix it.

## Types of asset whitelists

Each type of identity data is kept in a separate whitelist. The following table shows the reference collection name and type for each type of identity asset data.

Table 32. Reference collection name for asset whitelist data

| Type of data                                                                           | Reference collection name              | Reference collection type        |
|----------------------------------------------------------------------------------------|----------------------------------------|----------------------------------|
| IP addresses                                                                           | Asset Reconciliation IPv4 Whitelist    | Reference Set [Set Type: IP]     |
| DNS host names                                                                         | Asset Reconciliation DNS Whitelist     | Reference Set [Set Type: ALNIC*] |
| NetBIOS host names                                                                     | Asset Reconciliation NetBIOS Whitelist | Reference Set [Set Type: ALNIC*] |
| MAC addresses                                                                          | Asset Reconciliation MAC Whitelist     | Reference Set [Set Type: ALNIC*] |
| * ALNIC is an alphanumeric type that can accommodate host name and MAC address values. |                                        |                                  |

## Related concepts

### Asset blacklists

An *asset blacklist* is a collection of data that IBM QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

## Updating the blacklists and whitelists using the RESTful API

You can use the IBM QRadar RESTful API to customize the content of the asset blacklists and whitelists.

### About this task

You must specify the exact name of the reference set that you want to view or update.

- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation MAC Blacklist
- Asset Reconciliation IPv4 Whitelist
- Asset Reconciliation DNS Whitelist
- Asset Reconciliation NetBIOS Whitelist
- Asset Reconciliation MAC Whitelist

## Procedure

1. Type the following URL in your web browser to access the RESTful API interface:

```
https://ConsoleIPaddress/api_doc
```

2. In the navigation pane on the left, find 4.0>/reference\_data >/sets > /{name}.
3. To view the contents of an asset blacklist or whitelist, follow these steps:
  - a) Click the **GET** tab and scroll down to the **Parameters** section.
  - b) In the **Value** field for the **Name** parameter, type the name of the asset blacklist or whitelist that you want to view.
  - c) Click **Try It Out** and view the results at the bottom of the screen.
4. To add a value to an asset blacklist or whitelist, follow these steps:
  - a) Click the **POST** tab and scroll down to the **Parameters** section.
  - b) Type in the values for the following parameters:

| Table 33. Parameters that are required to add new asset data |                                                                                                                                                                                       |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter name                                               | Parameter description                                                                                                                                                                 |
| name                                                         | Represents the name of the reference collection that you want to update.                                                                                                              |
| value                                                        | Represents the data item that you want to add to the asset blacklist or whitelist. Must exactly match the asset update values that are provided by the originating asset data source. |

c) Click **Try It Out** to add the new value to the asset whitelist or asset blacklist.

## What to do next

For more information about using the RESTful API to change the reference sets, see the *IBM QRadar API Guide*.

## Identity exclusion searches

Identity exclusion searches can be used to manage single assets that accumulate large volumes of similar identity information for known, valid reasons.

For example, log sources can provide large volumes of asset identity information to the asset database. They provide IBM QRadar with near real-time changes to asset information and they can keep your asset database current. But log sources are most often the source of asset growth deviations and other asset-related anomalies.

When a log source sends incorrect asset data to QRadar, try to fix the log source so that the data it sends is usable by the asset database. If the log source cannot be fixed, you can build an identity exclusion search that blocks the asset information from entering the asset database.

You can also use an identity exclusion search where Identity\_Username+Is Any Of + Anonymous Logon to ensure that you are not updating assets that are related to service accounts or automated services.

## Differences between identity exclusion searches and blacklists

While identity exclusion searches appear to have similar functionality to asset blacklists, there are significant differences.

Blacklists can specify only raw asset data, such as MAC addresses and host names, that is to be excluded. Identity exclusion searches filter out asset data based on search fields like log source, category, and event name.

Blacklists do not account for the type of data source that is providing the data, whereas identity exclusion searches can be applied to events only. Identity exclusion searches can block asset updates based on common event search fields, such as event type, event name, category, and log source.

## Advanced tuning of asset reconciliation exclusion rules

You can tune the Asset Reconciliation Exclusion rules to refine the definition of deviating asset growth in one or more of the rules.

For example, consider this normalized template from an Asset Reconciliation Exclusion rule.

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
 by the Local system and NOT when any of
 Identity Host Name are contained in any of
 Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
 Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
 and when at least N1 events are seen with the same
 Identity Host Name and different Identity IP in N2
```

This table lists the variables in the rule template that can be tuned and the result of the change. Avoid changing other variables in the template.

Table 34. Options for tuning the asset reconciliation rules

| Variable | Default value | Tuning result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N1       | 3             | <p>Tuning this variable to a lower value results in more data being added to the blacklist because fewer events with conflicting data are needed for the rule to fire.</p> <p>Tuning this variable to a higher value results in less data being added to the blacklist because more events with conflicting data are needed for the rule to fire.</p>                                                                                                                                                                                                                                                  |
| N2       | 2 hours       | <p>Tuning this variable to a lower value reduces the window of time in which N1 events must be seen for the rule to fire. The time required to observe matching data is decreased, which results in less data being added to the blacklist.</p> <p>Tuning this variable to a higher value increases the time in which N1 events must be seen for the rule to fire. The time to observe matching data is increased, which results in more data being added to the blacklist.</p> <p>Increasing the time period might impact system memory resources as data is tracked over longer periods of time.</p> |

The Asset Reconciliation Exclusion rules are system-wide rules. Changes to the rules affect the way that the rule behaves throughout the entire system.

## Applying different tuning for rules

It might be necessary to apply different tuning for rules in different parts of the system. To apply different tuning for rules, you must duplicate the Asset Reconciliation Exclusion rules that you want to tune and add one or more tests to constrain the rules so that you test only certain parts of the system. For example, you might want to create rules that test only networks, log sources, or event types.

## About this task

Always be cautious when you are adding new rules to the system because as some tasks and CRE rules might impact system performance. It might be beneficial to add the new rules to the top of each test stack to allow the system to bypass the remainder of the test logic whenever an asset update matches the criteria for the new rule.

## Procedure

1. Duplicate the rule.

- a) On the **Offenses** tab, click **Rules** and select the rule that you want to copy.
- b) Click **Actions > Duplicate**.

It can be helpful if the name of the new rule is indicative of the reason for duplicating it.

2. Add a test to the rule.

Determine a filter that you want to use to apply the rule only to a subset of system data. For example, you can add a test that matches only events from a specific log source.

3. Tune the variables of the rule to achieve the wanted behavior.

4. Update the original rule.

- a) Add the same test that you added to the duplicate rule to the original rule, but this time invert the rules AND and AND NOT operators.

Inverting the operators prevents events from being triggered in both rules.



## Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

As the Network security administrator, you manage a corporate network that includes a public wifi network segment where IP address leases are typically short and frequent. The assets on this segment of the network tend to be transient, primarily notebooks and hand-held devices that log in and out of the public wifi frequently. Commonly, a single IP address is used multiple times by different devices over a short time.

In the rest of your deployment, you have a carefully managed network that consists only of inventoried, well-named company devices. IP address leases are much longer in this part of the network, and IP addresses are accessed by authentication only. On this network segment, you want to know immediately when there are any asset growth deviations and you want to keep the default settings for the asset reconciliation exclusion rules.

### Blacklisting IP addresses

In this environment, the default asset reconciliation exclusion rules inadvertently blacklist the entire network in a short time.

Your security team finds the asset-related notifications that are generated by the wifi segment are a nuisance. You want to prevent the wifi from triggering any more deviating asset growth notifications.

### Tuning asset reconciliation rules to ignore some asset updates

You review the **Asset deviation by log source** report in the last system notification. You determine that the blacklisted data is coming from the DHCP server on your wifi.

The values in the **Event Count** column, **Flow Count** column and the **Offenses** column for the row corresponding to the **AssetExclusion: Exclude IP By MAC Address** rule indicate that your wifi DHCP server is triggering this rule.

You add a test to the existing asset reconciliation exclusion rules to stop rules from adding wifi data to the blacklist.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

The updated rule tests only the events from the log sources that are not on your wifi DHCP server. To prevent wifi DHCP events from undergoing more expensive reference set and behavior analysis tests, you also moved this test to the top of the test stack.

## Clean up asset data after growth deviations

IBM QRadar uses the asset model to connect offenses in your deployment to physical or virtual assets in your network. The ability to collect and view relevant data on how assets are used is an important step in resolving security issues. It is important to maintain the asset database to ensure that the data is current and accurate.

Whether you fix the source of the problem or block the asset updates, you must clean up the asset database by removing the invalid asset data and removing the asset blacklist entries.

## Deleting blacklist entries

After you fixed the cause of the blacklist entries, you must clean up the remnant entries. You can remove the individual blacklist entries, however it is better to purge all blacklist entries and allow the blacklist values that are unrelated to the asset growth deviation to regenerate.

### Procedure

To purge a blacklist by using the IBM QRadar Console:

- a) On the navigation menu (☰), click **Admin**.
- b) In the **System Configuration** section, click **Reference Set Management**.
- c) Select a reference set and then click **Delete**.
- d) Use the quick search text box to search for the reference sets that you want to delete, and then click **Delete Listed**.

### Results

Purging a blacklist removes all blacklist entries, including those entries that were added manually. Blacklist entries that were manually added must be added again.

---

## Chapter 16. Event store and forward

Use the Store and Forward feature to manage schedules for forwarding events from your dedicated Event Collector appliances to Event Processor components in your deployment.

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590. For more information about these appliances, see the *IBM QRadar Hardware Guide*.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that is connected to QRadar.

You can schedule a time range for when you want the Event Collector to forward events to the Event Processor. By forwarding the events during non-business hours, you can ensure that the transmission does not negatively affect your network bandwidth. When event forwarding is scheduled, the events are stored locally on the Event Collector until the forwarding schedule kicks in. During this time, you cannot view the events in the IBM QRadar Console.

### **Related concepts**

[Capabilities in your IBM QRadar product](#)



---

## Chapter 17. Security content

You use the content management tools in IBM QRadar to import security content such as rules, reports, dashboards and applications into QRadar. Security content can come from other QRadar systems, or it can be developed independently to extend existing QRadar capabilities.

### **Related concepts**

[Capabilities in your IBM QRadar product](#)

---

## Types of security content

IBM QRadar content is bundled into two types: content packs and extensions.

### **Content packs**

Security *content packs* contain enhancements to specific types of security content. Often, they include content for third-party integrations or operating systems. For example, a security content pack for a third-party integration might contain new custom event properties that make information in the event payload searchable for the log source and available for reporting.

Security content packs are available from IBM Fix Central (<http://www.ibm.com/support/fixcentral>). Content packs are not available as part of an auto-update.

### **Extensions**

IBM and other vendors write security *extensions* that enhance or extend QRadar capabilities. An extension can contain apps, content items, such as custom rules, report templates, saved searches, or contain updates to existing content items. For example, an extension might include an app to add a tab in QRadar that provides visualizations for an offense.

On IBM Security App Exchange, extensions are known as apps. You can download QRadar apps from IBM Security App Exchange and use the **Extensions Management** tool to install them. Apps are not available as part of an auto-update.

### **Sources of security content**

QRadar content is available from the following sources:

#### **IBM Security App Exchange**

[IBM Security App Exchange](https://apps.xforce.ibmcloud.com) (<https://apps.xforce.ibmcloud.com>) is an app store and portal where you can browse and download QRadar extensions. It is a new way to share code, visualizations, reports, rules, and applications.

#### **IBM Fix Central**

[IBM Fix Central](http://www.ibm.com/support/fixcentral) ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)) provides fixes and updates to your system software, hardware, and operating system. You can download security content packs and extensions from IBM Fix Central.

#### **QRadar deployments**

You export custom content from a QRadar deployment as an extension and then import it into another system when you want to reuse the content. For example, you can export content from your development environment to your production environment. You can use the content management script to export all content, or you can choose to export only some custom content.

## Methods of importing and exporting content

---

You can use the following tools to import and export content in your IBM QRadar deployment.

### Extensions Management tool

Use the **Extensions Management** tool to add extensions to your QRadar deployment. When you import content by using the **Extensions Management** tool, you can view the content before it is installed. If the content items exist in your system, you can specify whether to replace the content item or skip the update.

You cannot use the **Extensions Management** tool to export content.

### Content management script

Use the content management script to export custom content from your QRadar deployment into an external, portable format. You can then use the script to import the custom content into another QRadar deployment. The script is useful when you want to automate moving content between your QRadar deployments.

The `contentManagement.pl` script is in the `/opt/qradar/bin` directory.

You must use the content management script to export content from the QRadar source deployment. You can use either the content management script or the **Extensions Management** tool to import the content to the target deployment.

### DSM Editor

In QRadar V7.3.3 and later, you can export your custom content that you create in the DSM Editor. Click the **Export** button in the DSM Editor to export your content from one QRadar deployment to another, or to external media.

**Note:** You can export content from an earlier version of QRadar and import into a later version. However, you cannot import content from a later version into an earlier version.

**Note:** If you move overridden rules from one QRadar deployment to another, use the **Replace Existing Content Items** option to ensure that the rules are imported correctly.

## Installing extensions by using Extensions Management

Use the **Extensions Management** tool to add security extensions to IBM QRadar. The **Extensions Management** tool allows you to view the content items in the extension and specify the method of handling content updates before you install the extension.

### Before you begin

Extensions must be on your local computer before you install them in QRadar.

You can download QRadar extensions from the IBM Security App Exchange (<https://apps.xforce.ibmcloud.com/>) and from IBM [Fix Central](http://www.ibm.com/support/fixcentral/) ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)).

### About this task

An extension is a bundle of QRadar functions. An extension can include content such as rules, reports, searches, reference sets, and dashboards. It can also include applications that enhance QRadar functions.

### Procedure

1. On the navigation menu (☰), click **Admin**.

2. In the **System Configuration** section, click **Extensions Management**.
3. To upload a new extension to the QRadar console, follow these steps:
  - a) Click **Add**.
  - b) Click **Browse** and navigate to find the extension.
  - c) Click **Install immediately** to install the extension without viewing the contents. Go to [“5.b” on page 141](#).
  - d) Click **Add**.
4. To view the contents of the extension, select it from the extensions list and click **More Details**.
5. To install the extension, follow these steps:
  - a) Select the extension from the list and click **Install**.
  - b) To assign a user to the app, select the **User Selection** menu, and select a user.  
For example, you might want to associate the app with a specified user that is listed in the **User Selection** menu who has the defined permissions.

**Note:**

This screen appears only if any of the apps in the extension that you are installing are configured to request authentication for background processes.

  - c) If the extension does not include a digital signature, or it is signed but the signature is not associated with the IBM Security Certificate Authority (CA), you must confirm that you still want to install it. Click **Install** to proceed with the installation.
  - d) Review the changes that the installation makes to the system.
  - e) Select **Preserve Existing Items** or **Replace Existing Items** to specify how to handle existing content items.

**Note:** If the extension contains overridden system rules, select **Replace Existing Items** to ensure that the rules are imported correctly.

  - f) Click **Install**.
  - g) Review the installation summary and click **OK**.

## Uninstalling a content extension

Remove a content extension that isn't useful anymore or that adversely impacts the system. You can remove rules, custom properties, reference data, and saved searches. You might not be able to remove some content if another content item depends on it.

### About this task

When you uninstall a content extension, any rules, custom properties, and reference data that were installed by the content extension are removed or reverted to their previous state. Saved searches can't be reverted. They can only be removed.

For example, if you've edited custom rules in an app that you now want to uninstall, you can preserve the changes you made for each customized rule. If the custom rule previously existed on the system, you can revert the rule to its previous state. If the custom rule didn't previously exist, you can remove it.

#### Note:

If you have introduced an outside dependency on a content extension that is installed by the app, QRadar doesn't remove that piece of content when you uninstall the app. For example, if you create a custom rule that uses one of the app's custom properties, that custom property isn't removed when you uninstall the app.

### Procedure

1. On the navigation menu (  ), click **Admin**.

2. In the **System Configuration** section, click **Extensions Management**.
3. Select the extension that you want to uninstall and click **Uninstall**.  
QRadar checks for any applications, rules, custom properties, reference data, and saved searches that are installed by the content extension that can be removed.
4. If you have manually altered any rules, custom properties, or reference data after you installed the app, choose whether to **Preserve** or **Remove/Revert** that content extension.
5. Click **Uninstall**, and then click **OK**.

## Content type identifiers for exporting custom content

When you export a specific type of custom content from IBM QRadar, you must specify the content type. You must use either the text identifier or the numeric identifier for the content type.

When you export content from a QRadar appliance, the content management script checks content dependencies, and then includes associated content in the export.

For example, when the content management script detects that a saved search is associated with a report that you want to export, the saved search is also exported. You can't export offense, asset, or vulnerability saved searches.

You use the content type identifier when you want to export all custom content of a specific type. If you want to export a specific content item from your QRadar deployment, you must know the unique identifier for that specific content item.

The following table describes the content type identifiers that are passed into the `contentManagement.pl` script for the `-c` parameter.

| <i>Table 35. Content type identifiers for exporting custom content</i> |                             |                           |
|------------------------------------------------------------------------|-----------------------------|---------------------------|
| <b>Custom content type</b>                                             | <b>Text identifier</b>      | <b>Numeric identifier</b> |
| All custom content                                                     | <b>all</b>                  | Not applicable            |
| Custom list of content                                                 | <b>package</b>              | Not applicable            |
| Dashboards                                                             | <b>dashboard</b>            | 4                         |
| Reports                                                                | <b>report</b>               | 10                        |
| Saved searches                                                         | <b>search</b>               | 1                         |
| FGroups <sup>1</sup>                                                   | <b>fgroup</b>               | 12                        |
| FGroup types                                                           | <b>fgrouptype</b>           | 13                        |
| Custom rules                                                           | <b>customrule</b>           | 3                         |
| Custom properties                                                      | <b>customproperty</b>       | 6                         |
| Log sources                                                            | <b>sensordevice</b>         | 17                        |
| Log source types                                                       | <b>sensordevicetype</b>     | 24                        |
| Log source categories                                                  | <b>sensordevicecategory</b> | 18                        |
| Log source extensions                                                  | <b>deviceextension</b>      | 16                        |
| Reference data collections                                             | <b>referencedata</b>        | 28                        |
| Custom QID map entries                                                 | <b>qidmap</b>               | 27                        |
| Historical correlation profiles                                        | <b>historicalsearch</b>     | 25                        |
| Custom functions                                                       | <b>custom_function</b>      | 77                        |
| Custom actions                                                         | <b>custom_action</b>        | 78                        |



| <i>Table 35. Content type identifiers for exporting custom content (continued)</i>                         |                              |                           |
|------------------------------------------------------------------------------------------------------------|------------------------------|---------------------------|
| <b>Custom content type</b>                                                                                 | <b>Text identifier</b>       | <b>Numeric identifier</b> |
| Applications                                                                                               | <b>installed_application</b> | 100                       |
| <sup>1</sup> An FGroup is a group of content such as a log source group, reporting group, or search group. |                              |                           |



---

## Chapter 18. SNMP trap configuration

IBM QRadar uses the Net-SNMP agent, which supports various system resource monitoring MIBs. They can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information about Net-SNMP, see Net-SNMP documentation.

In IBM QRadar, you can configure a rule to generate a rule response that sends an SNMP trap when configured conditions are met. QRadar acts as an agent to send the SNMP traps to another system.

A Simple Network Management Protocol (SNMP) trap is an event or offense notification that QRadar sends to a configured SNMP host for additional processing.

Customize the SNMP configuration parameters in the custom rules wizard and modify the SNMP traps that the custom rule engine sends to other software for management. QRadar provides two default traps. However, you can add custom traps or modify the existing traps to use new parameters.

For more information on SNMP, go to the [The Internet Engineering Task Force](http://www.ietf.org/) (<http://www.ietf.org/>) website and type RFC 1157 in the search field.

### **Related concepts**

[Capabilities in your IBM QRadar product](#)



---

## Chapter 19. Sensitive data protection

Configure a data obfuscation profile to prevent unauthorized access to sensitive or personal identifiable information in IBM QRadar.

*Data obfuscation* is the process of strategically hiding data from QRadar users. You can hide custom properties, normalized properties such as user names, or you can hide the content of a payload, such as credit card or social security numbers.

The expressions in the data obfuscation profile are evaluated against the payload and normalized properties. If the data matches the obfuscation expression, the data is hidden in QRadar. The data might be hidden to all users, or only to users belonging to particular domains or tenants. Affected users who try to query the database directly can't see the sensitive data. The data must be reverted to the original form by uploading the private key that was generated when the data obfuscation profile was created.

To ensure that QRadar can still correlate the hidden data values, the obfuscation process is deterministic. It displays the same set of characters each time the data value is found.

### **Related concepts**

[Capabilities in your IBM QRadar product](#)

---

## How does data obfuscation work?

Before you configure data obfuscation in your IBM QRadar deployment, you must understand how it works for new and existing offenses, assets, rules, and log source extensions.

### **Existing event data**

When a data obfuscation profile is enabled, the system masks the data for each event as it is received by QRadar. Events that are received by the appliance before data obfuscation is configured remain in the original unobfuscated state. The older event data is not masked and users can see the information.

### **Assets**

When data obfuscation is configured, the asset model accumulates data that is masked while the pre-existing asset model data remains unmasked.

To prevent someone from using unmasked data to trace the obfuscated information, purge the asset model data to remove the unmasked data. QRadar will repopulate the asset database with obfuscated values.

### **Offenses**

To ensure that offenses do not display data that was previously unmasked, close all existing offenses by resetting the SIM model. For more information, see [“Resetting SIM” on page 24](#).

### **Rules**

You must update rules that depend on data that was previously unmasked. For example, rules that are based on a specific user name do not fire when the user name is obfuscated.

### **Log source extensions**

Log source extensions that change the format of the event payload can cause issues with data obfuscation.

## Data obfuscation profiles

The data obfuscation profile contains information about which data to mask. It also tracks the keystore that is required to decrypt the data.

### Enabled profiles

Enable a profile only when you are sure that the expressions correctly target the data that you want to obfuscate. If you want to test the regular expression before you enable the data obfuscation profile, you can create a regex-based custom property.

A profile that is enabled immediately begins obfuscating data as defined by the enabled expressions in the profile. The enabled profile is automatically locked. Only the user who has the private key can disable or change the profile after it is enabled.

To ensure that obfuscated data can be traced back to an obfuscation profile, you cannot delete a profile that was enabled, even after you disable it.

### Locked profiles

A profile is automatically locked when you enable it, or you can lock it manually.

A locked profile has the following restrictions:

- You cannot edit it.
- You cannot enable or disable it. You must provide the keystore and unlock the profile before you can change it.
- You cannot delete it, even after it is unlocked.
- If a keystore is used with a profile that is locked, all other profiles that use that keystore are automatically locked.

The following table shows examples of profiles that are locked or unlocked:

| Table 36. Locked profile examples                                                                                                                           |                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Scenario                                                                                                                                                    | Result                                                |
| Profile A is locked. It was created by using keystore A.<br>Profile B is also created by using keystore A.                                                  | Profile B is automatically locked.                    |
| Profile A is created and enabled.                                                                                                                           | Profile A is automatically locked.                    |
| Profile A, Profile B, and Profile C are currently locked. All were created by using keystore A.<br>Profile B is selected and <b>Lock/Unlock</b> is clicked. | Profile A, Profile B, and Profile C are all unlocked. |

## Data obfuscation expressions

Data obfuscation expressions identify the data to hide. You can create data obfuscation expressions that are based on field-based properties or you can use regular expressions.

### Field-based properties

Use a field-based property to hide user names, group names, host names, and NetBIOS names. Expressions that use field-based properties obfuscate all instances of the data string. The data is hidden regardless of its log source, log source type, event name, or event category.

If the same data value exists in more than one of the fields, the data is obfuscated in all fields that contain the data even if you configured the profile to obfuscate only one of the four fields. For example, if you have a host name that is called IBMHost and a group name that is called IBMHost, the value IBMHost is obfuscated in both the host name field and the group name field even if the data obfuscation profile is configured to obfuscate only host names.

## Regular expressions

Use a regular expression to obfuscate one data string in the payload. The data is hidden only if it matches the log source, log source type, event name, or category that is defined in the expression.

You can use high-level and low-level categories to create a regular expression that is more specific than a field-based property. For example, you can use the following regex patterns to parse user names:

| Table 37. Regex user name parsing                                                                                                |                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Example regex patterns                                                                                                           | Matches                                                                                                                                  |
| <code>userName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*(?:[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])?)+[a-zA-Z]{2,20})\$</code>                    | john_smith@EXAMPLE.com,<br>jon@example.com,<br>jon@us.example.com                                                                        |
| <code>userName=(^([\w]+[^\W]))([^\W]\.?)([\w]+[^\W]\$)</code>                                                                    | john.smith, John.Smith,<br>john, jon_smith                                                                                               |
| <code>userName=^[a-zA-Z][a-zA-Z_-]*[\w_-]*[\S]\$ ^[a-zA-Z][0-9_-]*[\S]\$ ^[a-zA-Z]*[\S]\$</code>                                 | johnsmith, Johnsmith123,<br>john_smith123,<br>john123_smith, john-smith                                                                  |
| <code>userName=(/S+)</code>                                                                                                      | Matches any non-white space after the equal, =, sign. This regular expression is non-specific and can lead to system performance issues. |
| <code>msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*)@b((?:[01]?[d]?[d] 2[0-4][d] 25[0-5])\.){3}([01]?[d]?[d] 2[0-4][d] 25[0-5])\b</code> | Matches users with IP address. For example, john.smith@192.0.2.0                                                                         |
| <code>src=b((?:[01]?[d]?[d] 2[0-4][d] 25[0-5])\.){3}([01]?[d]?[d] 2[0-4][d] 25[0-5])\b</code>                                    | Matches IP address formats.                                                                                                              |
| <code>host=^(([a-zA-Z0-9] [a-zA-Z0-9][a-zA-Z0-9\-.]*[a-zA-Z0-9])\.)*([A-Za-z0-9] [A-Za-z0-9][A-Za-z0-9\-.]*[A-Za-z0-9])\$</code> | hostname.example.com,<br>hostname.co.uk                                                                                                  |

## Scenario: Obfuscating user names

You are an IBM QRadar administrator. Your organization has an agreement with the workers union that all personal identifiable information must be hidden from QRadar users. You want to configure QRadar to hide all user names.

Use the **Data Obfuscation Management** feature on the **Admin** tab to configure QRadar to hide the data:

1. Create a data obfuscation profile and download the system-generated private key. Save the key in a secure location.
2. Create the data obfuscation expressions to target the data that you want to hide.
3. Enable the profile so that the system begins to obfuscate the data.
4. To read the data in QRadar, upload the private key to deobfuscate the data.

## Creating a data obfuscation profile

IBM QRadar uses data obfuscation profiles to determine which data to mask, and to ensure that the correct keystore is used to unmask the data.

### About this task

You can create a profile that creates a new keystore or you can use an existing keystore. If you create a keystore, it must be downloaded and stored in a secure location. Remove the keystore from the local system and store it in a location that can be accessed only by users who are authorized to view the unmasked data.

Configuring profiles that use different keystores is useful when you want to limit data access to different groups of users. For example, create two profiles that use different keystores when you want one group of users to see user names and another group of users to see host names.

### Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, click **Data Obfuscation Management**.
3. To create a new profile, click **Add** and type a unique name and description for the profile.
4. To create a new keystore for the profile, complete these steps:
  - a) Click **System generate keystore**.
  - b) In the **Provider** list box, select **IBMJCE**.
  - c) In the **Algorithm** list box, select **JCE** and select whether to generate 512-bit or 1024-bit encryption keys.  
In the **Keystore Certificate CN** box, the fully qualified domain name for the QRadar server is auto-populated.
  - d) In the **Keystore password** box, enter the keystore password.  
The keystore password is required to protect the integrity of the keystore. The password must be at least 8 characters in length.
  - e) In the **Verify keystore password**, retype the password.
5. To use an existing keystore with the profile, complete these steps:
  - a) Click **Upload keystore**.
  - b) Click **Browse** and select the keystore file.
  - c) In the **Keystore password** box, type the password for the keystore.
6. Click **Submit**.
7. Download the keystore.  
Remove the keystore from your system and store it in a secure location.

### What to do next

[Create the data obfuscation expressions](#) that target the data that you want to hide.

## Creating data obfuscation expressions

The data obfuscation profile uses expressions to specify which data to hide from IBM QRadar users. The expressions can use either field-based properties or regular expressions.

### About this task


After an expression is created, you cannot change the type. For example, you cannot create a property-based expression and then later change it to a regular expression.



You cannot hide a normalized numeric field, such as port number or an IP address.

Multiple expressions that hide the same data cause data to be hidden twice. To decrypt data that is hidden multiple times, each keystore that is used in the obfuscation process must be applied in the order that the obfuscation occurred.

## Procedure

1. On the navigation menu (  ), click **Admin**.
2. In the **Data Sources** section, click **Data Obfuscation Management**.
3. Click the profile that you want to configure, and click **View Contents**.  
You cannot configure profiles that are locked.
4. To create a new data obfuscation expression, click **Add** and type a unique name and description for the profile.
5. Select the **Enabled** check box to enable the profile.
6. Optional: To apply the obfuscation expression to specific domains or tenants, select them from the **Domain** field. Or select **All Domains** to apply the obfuscation expression to all domains and tenants.
7. To create a field-based expression, click **Field Based** and select the field type to obfuscate.
8. To create a regular expression, click **RegEx** and configure the regEx properties.
9. Click **Save**.

## Deobfuscating data so that it can be viewed in the console

When data obfuscation is configured on an IBM QRadar system, the masked version of the data is shown throughout the application. You must have both the corresponding keystore and the password to deobfuscate the data so that it can be viewed.

### Before you begin

You must be an administrator and have the private key and the password for the key before you can deobfuscate data. The private key must be on your local computer.

### About this task

Before you can see the obfuscated data, you must upload the private key. After the key is uploaded, it remains available on the system for the duration of the current session. The session ends when you log out of QRadar, when the cache is cleared on the QRadar Console, or when there is an extended period of inactivity. When the session ends, the private keys that were uploaded in the previous session are no longer visible.

QRadar can use the keys available in the current session to automatically deobfuscate data. With auto-deobfuscation enabled, you do not have to repeatedly select the private key on the **Obfuscation Session Key** window each time that you want to view the data. Auto-deobfuscate is automatically disabled when the current session ends.

## Procedure

1. On the **Event Details** page, find the data that you want to deobfuscate.
2. To deobfuscate identity-based data:
  - a) Click the lock icon next to the data that you want to deobfuscate.
  - b) In the **Upload Key** section, click **Select File** and select the keystore to upload.
  - c) In the **Password** box, type the password that matches the keystore.
  - d) Click **Upload**.

The **Deobfuscation** window shows the event payload, the profile names that are associated with the keystore, the obfuscated text, and the deobfuscated text.

- e) Optional: Click **Toggle Auto Deobfuscate** to enable auto-deobfuscation.

After you toggle the auto-deobfuscation setting, you must refresh the browser window and reload the event details page for the changes to appear.

- 3. To deobfuscate payload data that is not identity-based:

- a) On the toolbar on the **Event Details** page, click **Obfuscation > Deobfuscation keys**.
- b) In the **Upload Key** section, click **Select File** and select the private key to upload.
- c) In the **Password** box, type the password that matches the private key and click **Upload**.
- d) In the **Payload information** box, select and copy the obfuscated text to the clipboard.
- e) On the toolbar on the **Event Details** page, click **Obfuscation > Deobfuscation**.
- f) Paste the obfuscated text in to dialog box.
- g) Select the obfuscation profile from the drop-down list and click **Deobfuscate**.

## Chapter 20. Event categories

Event categories are used to group incoming events for processing by IBM QRadar. The event categories are searchable and help you monitor your network.

Events that occur on your network are aggregated into high-level and low-level categories. Each high-level category contains low-level categories and an associated severity level and ID number.

You can review the severity levels that are assigned to events and adjust them to suit your corporate policy needs.

You can run an AQL query by using high-level and low-level event category IDs. The category IDs for the associated category names can be retrieved from the event category tables.

For example, if you are developing applications on QRadar, you can run an AQL search similar to the following query from the command line, to gather data from Ariel:

```
select qidname(qid) as 'Event', username as 'Username', devicetime as 'Time'
from events where '<high-level category ID>' and '<Low-level category ID>' and
LOGSOURCENAME(logsourceid) like "%Low-level category name%" last 3 days
```

### Related concepts

[Capabilities in your IBM QRadar product](#)

## High-level event categories

Events in IBM QRadar log sources are grouped into high-level categories. Each event is assigned to a specific high-level category.

Categorizing the incoming events ensures that you can easily search the data.

The following table describes the high-level event categories.

| Table 38. High-level event categories        |             |                                                                                                                                                                                   |
|----------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category                                     | Category ID | Description                                                                                                                                                                       |
| <a href="#">“Recon” on page 154</a>          | 1000        | Events that are related to scanning and other techniques that are used to identify network resources, for example, network or host port scans.                                    |
| <a href="#">“DoS” on page 156</a>            | 2000        | Events that are related to denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.       |
| <a href="#">“Authentication” on page 159</a> | 3000        | Events that are related to authentication controls, group, or privilege change, for example, log in or log out.                                                                   |
| <a href="#">“Access” on page 168</a>         | 4000        | Events resulting from an attempt to access network resources, for example, firewall accept or deny.                                                                               |
| <a href="#">“Exploit” on page 170</a>        | 5000        | Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.                                           |
| <a href="#">“Malware” on page 172</a>        | 6000        | Events that are related to viruses, trojans, back door attacks, or other forms of hostile software. Malware events might include a virus, trojan, malicious software, or spyware. |

| <i>Table 38. High-level event categories (continued)</i> |             |                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category                                                 | Category ID | Description                                                                                                                                                                                                                                               |
| <a href="#">“Suspicious Activity” on page 173</a>        | 7000        | The nature of the threat is unknown but behavior is suspicious. The threat might include protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known intrusion detection system (IDS) evasion techniques. |
| <a href="#">“System” on page 178</a>                     | 8000        | Events that are related to system changes, software installation, or status messages.                                                                                                                                                                     |
| <a href="#">“Policy” on page 183</a>                     | 9000        | Events regarding corporate policy violations or misuse.                                                                                                                                                                                                   |
| <a href="#">“Unknown” on page 185</a>                    | 10000       | Events that are related to unknown activity on your system.                                                                                                                                                                                               |
| <a href="#">“CRE” on page 186</a>                        | 12000       | Events that are generated from an offense or event rule.                                                                                                                                                                                                  |
| <a href="#">“Potential Exploit” on page 186</a>          | 13000       | Events relate to potential application exploits and buffer overflow attempts.                                                                                                                                                                             |
| <a href="#">Flow</a>                                     | 14000       | Events that are related to flow actions.                                                                                                                                                                                                                  |
| <a href="#">“User Defined” on page 189</a>               | 15000       | Events that are related to user-defined objects.                                                                                                                                                                                                          |
| <a href="#">“SIM Audit” on page 192</a>                  | 16000       | Events that are related to user interaction with the Console and administrative functions.                                                                                                                                                                |
| <a href="#">“VIS Host Discovery” on page 193</a>         | 17000       | Events that are related to the host, ports, or vulnerabilities that the VIS component discovers.                                                                                                                                                          |
| <a href="#">“Application” on page 193</a>                | 18000       | Events that are related to application activity.                                                                                                                                                                                                          |
| <a href="#">“Audit” on page 219</a>                      | 19000       | Events that are related to audit activity.                                                                                                                                                                                                                |
| <a href="#">“Control” on page 223</a>                    | 22000       | Events that are related to your hardware system.                                                                                                                                                                                                          |
| <a href="#">“Asset Profiler” on page 225</a>             | 23000       | Events that are related to asset profiles.                                                                                                                                                                                                                |
| <a href="#">Sense</a>                                    | 24000       | Events that are related to UBA.                                                                                                                                                                                                                           |

## Recon

The Recon category contains events that are related to scanning and other techniques that are used to identify network resources.

The following table describes the low-level event categories and associated severity levels for the Recon category.

| <i>Table 39. Low-level categories and severity levels for the Recon events category</i> |             |                                    |                         |
|-----------------------------------------------------------------------------------------|-------------|------------------------------------|-------------------------|
| Low-level event category                                                                | Category ID | Description                        | Severity level (0 - 10) |
| Unknown Form of Recon                                                                   | 1001        | An unknown form of reconnaissance. | 2                       |

*Table 39. Low-level categories and severity levels for the Recon events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                 | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------------------|--------------------------------|
| Application Query               | 1002               | Reconnaissance to applications on your system.                     | 3                              |
| Host Query                      | 1003               | Reconnaissance to a host in your network.                          | 3                              |
| Network Sweep                   | 1004               | Reconnaissance on your network.                                    | 4                              |
| Mail Reconnaissance             | 1005               | Reconnaissance on your mail system.                                | 3                              |
| Windows Reconnaissance          | 1006               | Reconnaissance for Windows operating system.                       | 3                              |
| Portmap / RPC r<br>\Request     | 1007               | Reconnaissance on your portmap or RPC request.                     | 3                              |
| Host Port Scan                  | 1008               | Indicates that a scan occurred on the host ports.                  | 4                              |
| RPC Dump                        | 1009               | Indicates that Remote Procedure Call (RPC) information is removed. | 3                              |
| DNS Reconnaissance              | 1010               | Reconnaissance on the DNS server.                                  | 3                              |
| Misc Reconnaissance Event       | 1011               | Miscellaneous reconnaissance event.                                | 2                              |
| Web Reconnaissance              | 1012               | Web reconnaissance on your network.                                | 3                              |
| Database Reconnaissance         | 1013               | Database reconnaissance on your network.                           | 3                              |
| ICMP Reconnaissance             | 1014               | Reconnaissance on ICMP traffic.                                    | 3                              |
| UDP Reconnaissance              | 1015               | Reconnaissance on UDP traffic.                                     | 3                              |
| SNMP Reconnaissance             | 1016               | Reconnaissance on SNMP traffic.                                    | 3                              |
| ICMP Host Query                 | 1017               | Indicates an ICMP host query.                                      | 3                              |
| UDP Host Query                  | 1018               | Indicates a UDP host query.                                        | 3                              |
| NMAP Reconnaissance             | 1019               | Indicates NMAP reconnaissance.                                     | 3                              |

Table 39. Low-level categories and severity levels for the Recon events category (continued)

| Low-level event category | Category ID | Description                                   | Severity level (0 - 10) |
|--------------------------|-------------|-----------------------------------------------|-------------------------|
| TCP Reconnaissance       | 1020        | Indicates TCP reconnaissance on your network. | 3                       |
| UNIX Reconnaissance      | 1021        | Reconnaissance on your UNIX network.          | 3                       |
| FTP Reconnaissance       | 1022        | Indicates FTP reconnaissance.                 | 3                       |

## DoS

The DoS category contains events that are related to denial-of-service (DoS) attacks against services or hosts.

The following table describes the low-level event categories and associated severity levels for the DoS category.

Table 40. Low-level categories and severity levels for the DoS events category

| Low-level event category | Category ID | Description                           | Severity level (0 - 10) |
|--------------------------|-------------|---------------------------------------|-------------------------|
| Unknown DoS Attack       | 2001        | Indicates an unknown DoS attack.      | 8                       |
| ICMP DoS                 | 2002        | Indicates an ICMP DoS attack.         | 9                       |
| TCP DoS                  | 2003        | Indicates a TCP DoS attack.           | 9                       |
| UDP DoS                  | 2004        | Indicates a UDP DoS attack.           | 9                       |
| DNS Service DoS          | 2005        | Indicates a DNS service DoS attack.   | 8                       |
| Web Service DoS          | 2006        | Indicates a web service DoS attack.   | 8                       |
| Mail Service DoS         | 2007        | Indicates a mail server DoS attack.   | 8                       |
| Distributed DoS          | 2008        | Indicates a distributed DoS attack.   | 9                       |
| Misc DoS                 | 2009        | Indicates a miscellaneous DoS attack. | 8                       |
| UNIX DoS                 | 2010        | Indicates a UNIX DoS attack.          | 8                       |
| Windows DoS              | 2011        | Indicates a Windows DoS attack.       | 8                       |
| Database DoS             | 2012        | Indicates a database DoS attack.      | 8                       |

Table 40. Low-level categories and severity levels for the DoS events category (continued)

| Low-level event category       | Category ID | Description                                                   | Severity level (0 - 10) |
|--------------------------------|-------------|---------------------------------------------------------------|-------------------------|
| FTP DoS                        | 2013        | Indicates an FTP DoS attack.                                  | 8                       |
| Infrastructure DoS             | 2014        | Indicates a DoS attack on the infrastructure.                 | 8                       |
| Telnet DoS                     | 2015        | Indicates a Telnet DoS attack.                                | 8                       |
| Brute Force Login              | 2016        | Indicates access to your system through unauthorized methods. | 8                       |
| High Rate TCP DoS              | 2017        | Indicates a high rate TCP DoS attack.                         | 8                       |
| High Rate UDP DoS              | 2018        | Indicates a high rate UDP DoS attack.                         | 8                       |
| High Rate ICMP DoS             | 2019        | Indicates a high rate ICMP DoS attack.                        | 8                       |
| High Rate DoS                  | 2020        | Indicates a high rate DoS attack.                             | 8                       |
| Medium Rate TCP DoS            | 2021        | Indicates a medium rate TCP attack.                           | 8                       |
| Medium Rate UDP DoS            | 2022        | Indicates a medium rate UDP attack.                           | 8                       |
| Medium Rate ICMP DoS           | 2023        | Indicates a medium rate ICMP attack.                          | 8                       |
| Medium Rate DoS                | 2024        | Indicates a medium rate DoS attack.                           | 8                       |
| Low Rate TCP DoS               | 2025        | Indicates a low rate TCP DoS attack.                          | 8                       |
| Low Rate UDP DoS               | 2026        | Indicates a low rate UDP DoS attack.                          | 8                       |
| Low Rate ICMP DoS              | 2027        | Indicates a low rate ICMP DoS attack.                         | 8                       |
| Low Rate DoS                   | 2028        | Indicates a low rate DoS attack.                              | 8                       |
| Distributed High Rate TCP DoS  | 2029        | Indicates a distributed high rate TCP DoS attack.             | 8                       |
| Distributed High Rate UDP DoS  | 2030        | Indicates a distributed high rate UDP DoS attack.             | 8                       |
| Distributed High Rate ICMP DoS | 2031        | Indicates a distributed high rate ICMP DoS attack.            | 8                       |

Table 40. Low-level categories and severity levels for the DoS events category (continued)

| Low-level event category         | Category ID | Description                                          | Severity level (0 - 10) |
|----------------------------------|-------------|------------------------------------------------------|-------------------------|
| Distributed High Rate DoS        | 2032        | Indicates a distributed high rate DoS attack.        | 8                       |
| Distributed Medium Rate TCP DoS  | 2033        | Indicates a distributed medium rate TCP DoS attack.  | 8                       |
| Distributed Medium Rate UDP DoS  | 2034        | Indicates a distributed medium rate UDP DoS attack.  | 8                       |
| Distributed Medium Rate ICMP DoS | 2035        | Indicates a distributed medium rate ICMP DoS attack. | 8                       |
| Distributed Medium Rate DoS      | 2036        | Indicates a distributed medium rate DoS attack.      | 8                       |
| Distributed Low Rate TCP DoS     | 2037        | Indicates a distributed low rate TCP DoS attack.     | 8                       |
| Distributed Low Rate UDP DoS     | 2038        | Indicates a distributed low rate UDP DoS attack.     | 8                       |
| Distributed Low Rate ICMP DoS    | 2039        | Indicates a distributed low rate ICMP DoS attack.    | 8                       |
| Distributed Low Rate DoS         | 2040        | Indicates a distributed low rate DoS attack.         | 8                       |
| High Rate TCP Scan               | 2041        | Indicates a high rate TCP scan.                      | 8                       |
| High Rate UDP Scan               | 2042        | Indicates a high rate UDP scan.                      | 8                       |
| High Rate ICMP Scan              | 2043        | Indicates a high rate ICMP scan.                     | 8                       |
| High Rate Scan                   | 2044        | Indicates a high rate scan.                          | 8                       |
| Medium Rate TCP Scan             | 2045        | Indicates a medium rate TCP scan.                    | 8                       |
| Medium Rate UDP Scan             | 2046        | Indicates a medium rate UDP scan.                    | 8                       |
| Medium Rate ICMP Scan            | 2047        | Indicates a medium rate ICMP scan.                   | 8                       |
| Medium Rate Scan                 | 2048        | Indicates a medium rate scan.                        | 8                       |
| Low Rate TCP Scan                | 2049        | Indicates a low rate TCP scan.                       | 8                       |



| <i>Table 40. Low-level categories and severity levels for the DoS events category (continued)</i> |                    |                                                             |                                |
|---------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                   | <b>Category ID</b> | <b>Description</b>                                          | <b>Severity level (0 - 10)</b> |
| Low Rate UDP Scan                                                                                 | 2050               | Indicates a low rate UDP scan.                              | 8                              |
| Low Rate ICMP Scan                                                                                | 2051               | Indicates a low rate ICMP scan.                             | 8                              |
| Low Rate Scan                                                                                     | 2052               | Indicates a low rate scan.                                  | 8                              |
| VoIP DoS                                                                                          | 2053               | Indicates a VoIP DoS attack.                                | 8                              |
| Flood                                                                                             | 2054               | Indicates a Flood attack.                                   | 8                              |
| TCP Flood                                                                                         | 2055               | Indicates a TCP flood attack.                               | 8                              |
| UDP Flood                                                                                         | 2056               | Indicates a UDP flood attack.                               | 8                              |
| ICMP Flood                                                                                        | 2057               | Indicates an ICMP flood attack.                             | 8                              |
| SYN Flood                                                                                         | 2058               | Indicates a SYN flood attack.                               | 8                              |
| URG Flood                                                                                         | 2059               | Indicates a flood attack with the urgent (URG) flag on.     | 8                              |
| SYN URG Flood                                                                                     | 2060               | Indicates a SYN flood attack with the urgent (URG) flag on. | 8                              |
| SYN FIN Flood                                                                                     | 2061               | Indicates a SYN FIN flood attack.                           | 8                              |
| SYN ACK Flood                                                                                     | 2062               | Indicates a SYN ACK flood attack.                           | 8                              |

## Authentication

The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

The following table describes the low-level event categories and associated severity levels for the authentication category.

| <i>Table 41. Low-level categories and severity levels for the authentication events category</i> |                    |                                    |                                |
|--------------------------------------------------------------------------------------------------|--------------------|------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                  | <b>Category ID</b> | <b>Description</b>                 | <b>Severity level (0 - 10)</b> |
| Unknown Authentication                                                                           | 3001               | Indicates unknown authentication.  | 1                              |
| Host Login Succeeded                                                                             | 3002               | Indicates a successful host login. | 1                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b>                   | <b>Category ID</b> | <b>Description</b>                                                                      | <b>Severity level (0 - 10)</b> |
|---------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------|--------------------------------|
| Host Login Failed                                 | 3003               | Indicates that the host login failed.                                                   | 3                              |
| Misc Login Succeeded                              | 3004               | Indicates that the login sequence succeeded.                                            | 1                              |
| Misc Login Failed                                 | 3005               | Indicates that login sequence failed.                                                   | 3                              |
| Privilege Escalation Failed                       | 3006               | Indicates that the privileged escalation failed.                                        | 3                              |
| Privilege Escalation Succeeded                    | 3007               | Indicates that the privilege escalation succeeded.                                      | 1                              |
| Mail Service Login Succeeded                      | 3008               | Indicates that the mail service login succeeded.                                        | 1                              |
| Mail Service Login Failed                         | 3009               | Indicates that the mail service login failed.                                           | 3                              |
| Auth Server Login Failed                          | 3010               | Indicates that the authentication server login failed.                                  | 3                              |
| Auth Server Login Succeeded                       | 3011               | Indicates that the authentication server login succeeded.                               | 1                              |
| Web Service Login Succeeded                       | 3012               | Indicates that the web service login succeeded.                                         | 1                              |
| Web Service Login Failed                          | 3013               | Indicates that the web service login failed.                                            | 3                              |
| Admin Login Successful                            | 3014               | Indicates that an administrative login was successful.                                  | 1                              |
| Admin Login Failure                               | 3015               | Indicates the administrative login failed.                                              | 3                              |
| Suspicious Username                               | 3016               | Indicates that a user attempted to access the network by using an incorrect user name.  | 4                              |
| Login with username/ password defaults successful | 3017               | Indicates that a user accessed the network by using the default user name and password. | 4                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b>                  | <b>Category ID</b> | <b>Description</b>                                                                                        | <b>Severity level (0 - 10)</b> |
|--------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------|
| Login with username/<br>password defaults failed | 3018               | Indicates that a user was unsuccessful accessing the network by using the default user name and password. | 4                              |
| FTP Login Succeeded                              | 3019               | Indicates that the FTP login was successful.                                                              | 1                              |
| FTP Login Failed                                 | 3020               | Indicates that the FTP login failed.                                                                      | 3                              |
| SSH Login Succeeded                              | 3021               | Indicates that the SSH login was successful.                                                              | 1                              |
| SSH Login Failed                                 | 3022               | Indicates that the SSH login failed.                                                                      | 2                              |
| User Right Assigned                              | 3023               | Indicates that user access to network resources was successfully granted.                                 | 1                              |
| User Right Removed                               | 3024               | Indicates that user access to network resources was successfully removed.                                 | 1                              |
| Trusted Domain Added                             | 3025               | Indicates that a trusted domain was successfully added to your deployment.                                | 1                              |
| Trusted Domain Removed                           | 3026               | Indicates that a trusted domain was removed from your deployment.                                         | 1                              |
| System Security Access Granted                   | 3027               | Indicates that system security access was successfully granted.                                           | 1                              |
| System Security Access Removed                   | 3028               | Indicates that system security access was successfully removed.                                           | 1                              |
| Policy Added                                     | 3029               | Indicates that a policy was successfully added.                                                           | 1                              |
| Policy Change                                    | 3030               | Indicates that a policy was successfully changed.                                                         | 1                              |
| User Account Added                               | 3031               | Indicates that a user account was successfully added.                                                     | 1                              |
| User Account Changed                             | 3032               | Indicates a change to an existing user account.                                                           | 1                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b>   | <b>Category ID</b> | <b>Description</b>                                                              | <b>Severity level (0 - 10)</b> |
|-----------------------------------|--------------------|---------------------------------------------------------------------------------|--------------------------------|
| Password Change Failed            | 3033               | Indicates that an attempt to change an existing password failed.                | 3                              |
| Password Change Succeeded         | 3034               | Indicates that a password change was successful.                                | 1                              |
| User Account Removed              | 3035               | Indicates that a user account was successfully removed.                         | 1                              |
| Group Member Added                | 3036               | Indicates that a group member was successfully added.                           | 1                              |
| Group Member Removed              | 3037               | Indicates that a group member was removed.                                      | 1                              |
| Group Added                       | 3038               | Indicates that a group was successfully added.                                  | 1                              |
| Group Changed                     | 3039               | Indicates a change to an existing group.                                        | 1                              |
| Group Removed                     | 3040               | Indicates that a group was removed.                                             | 1                              |
| Computer Account Added            | 3041               | Indicates that a computer account was successfully added.                       | 1                              |
| Computer Account Changed          | 3042               | Indicates a change to an existing computer account.                             | 1                              |
| Computer Account Removed          | 3043               | Indicates that a computer account was successfully removed.                     | 1                              |
| Remote Access Login Succeeded     | 3044               | Indicates that access to the network by using a remote login was successful.    | 1                              |
| Remote Access Login Failed        | 3045               | Indicates that an attempt to access the network by using a remote login failed. | 3                              |
| General Authentication Successful | 3046               | Indicates that the authentication processes was successful.                     | 1                              |
| General Authentication Failed     | 3047               | Indicates that the authentication process failed.                               | 3                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                 | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------------------------------|--------------------------------|
| Telnet Login Succeeded          | 3048               | Indicates that the telnet login was successful.                                    | 1                              |
| Telnet Login Failed             | 3049               | Indicates that the telnet login failed.                                            | 3                              |
| Suspicious Password             | 3050               | Indicates that a user attempted to log in by using a suspicious password.          | 4                              |
| Samba Login Successful          | 3051               | Indicates that a user successfully logged in by using Samba.                       | 1                              |
| Samba Login Failed              | 3052               | Indicates a user failed to log in by using Samba.                                  | 3                              |
| Auth Server Session Opened      | 3053               | Indicates that a communication session with the authentication server was started. | 1                              |
| Auth Server Session Closed      | 3054               | Indicates that a communication session with the authentication server was closed.  | 1                              |
| Firewall Session Closed         | 3055               | Indicates that a firewall session was closed.                                      | 1                              |
| Host Logout                     | 3056               | Indicates that a host successfully logged out.                                     | 1                              |
| Misc Logout                     | 3057               | Indicates that a user successfully logged out.                                     | 1                              |
| Auth Server Logout              | 3058               | Indicates that the process to log out of the authentication server was successful. | 1                              |
| Web Service Logout              | 3059               | Indicates that the process to log out of the web service was successful.           | 1                              |
| Admin Logout                    | 3060               | Indicates that the administrative user successfully logged out.                    | 1                              |
| FTP Logout                      | 3061               | Indicates that the process to log out of the FTP service was successful.           | 1                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                              | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------------------------------------------------|--------------------------------|
| SSH Logout                      | 3062               | Indicates that the process to log out of the SSH session was successful.                        | 1                              |
| Remote Access Logout            | 3063               | Indicates that the process to log out using remote access was successful.                       | 1                              |
| Telnet Logout                   | 3064               | Indicates that the process to log out of the Telnet session was successful.                     | 1                              |
| Samba Logout                    | 3065               | Indicates that the process to log out of Samba was successful.                                  | 1                              |
| SSH Session Started             | 3066               | Indicates that the SSH login session was initiated on a host.                                   | 1                              |
| SSH Session Finished            | 3067               | Indicates the termination of an SSH login session on a host.                                    | 1                              |
| Admin Session Started           | 3068               | Indicates that a login session was initiated on a host by an administrative or privileged user. | 1                              |
| Admin Session Finished          | 3069               | Indicates the termination of an administrator or privileged users login session on a host.      | 1                              |
| VoIP Login Succeeded            | 3070               | Indicates a successful VoIP service login                                                       | 1                              |
| VoIP Login Failed               | 3071               | Indicates an unsuccessful attempt to access VoIP service.                                       | 1                              |
| VoIP Logout                     | 3072               | Indicates a user logout,                                                                        | 1                              |
| VoIP Session Initiated          | 3073               | Indicates the beginning of a VoIP session.                                                      | 1                              |
| VoIP Session Terminated         | 3074               | Indicates the end of a VoIP session.                                                            | 1                              |
| Database Login Succeeded        | 3075               | Indicates a successful database login.                                                          | 1                              |
| Database Login Failure          | 3076               | Indicates a database login attempt failed.                                                      | 3                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b>  | <b>Category ID</b> | <b>Description</b>                                                          | <b>Severity level (0 - 10)</b> |
|----------------------------------|--------------------|-----------------------------------------------------------------------------|--------------------------------|
| IKE Authentication Failed        | 3077               | Indicates a failed Internet Key Exchange (IKE) authentication was detected. | 3                              |
| IKE Authentication Succeeded     | 3078               | Indicates that a successful IKE authentication was detected.                | 1                              |
| IKE Session Started              | 3079               | Indicates that an IKE session started.                                      | 1                              |
| IKE Session Ended                | 3080               | Indicates that an IKE session ended.                                        | 1                              |
| IKE Error                        | 3081               | Indicates an IKE error message.                                             | 1                              |
| IKE Status                       | 3082               | Indicates IKE status message.                                               | 1                              |
| RADIUS Session Started           | 3083               | Indicates that a RADIUS session started.                                    | 1                              |
| RADIUS Session Ended             | 3084               | Indicates a RADIUS session ended.                                           | 1                              |
| RADIUS Session Denied            | 3085               | Indicates that a RADIUS session was denied.                                 | 1                              |
| RADIUS Session Status            | 3086               | Indicates a RADIUS session status message.                                  | 1                              |
| RADIUS Authentication Failed     | 3087               | Indicates a RADIUS authentication failure.                                  | 3                              |
| RADIUS Authentication Successful | 3088               | Indicates a RADIUS authentication succeeded.                                | 1                              |
| TACACS Session Started           | 3089               | Indicates a TACACS session started.                                         | 1                              |
| TACACS Session Ended             | 3090               | Indicates a TACACS session ended.                                           | 1                              |
| TACACS Session Denied            | 3091               | Indicates that a TACACS session was denied.                                 | 1                              |
| TACACS Session Status            | 3092               | Indicates a TACACS session status message.                                  | 1                              |
| TACACS Authentication Successful | 3093               | Indicates a TACACS authentication succeeded.                                | 1                              |
| TACACS Authentication Failed     | 3094               | Indicates a TACACS authentication failure.                                  | 1                              |

*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b>  | <b>Category ID</b> | <b>Description</b>                                                 | <b>Severity level (0 - 10)</b> |
|----------------------------------|--------------------|--------------------------------------------------------------------|--------------------------------|
| Deauthenticating Host Succeeded  | 3095               | Indicates that the deauthentication of a host was successful.      | 1                              |
| Deauthenticating Host Failed     | 3096               | Indicates that the deauthentication of a host failed.              | 3                              |
| Station Authentication Succeeded | 3097               | Indicates that the station authentication was successful.          | 1                              |
| Station Authentication Failed    | 3098               | Indicates that the station authentication of a host failed.        | 3                              |
| Station Association Succeeded    | 3099               | Indicates that the station association was successful.             | 1                              |
| Station Association Failed       | 3100               | Indicates that the station association failed.                     | 3                              |
| Station Reassociation Succeeded  | 3101               | Indicates that the station reassociation was successful.           | 1                              |
| Station Reassociation Failed     | 3102               | Indicates that the station association failed.                     | 3                              |
| Disassociating Host Succeeded    | 3103               | Indicates that the disassociating a host was successful.           | 1                              |
| Disassociating Host Failed       | 3104               | Indicates that the disassociating a host failed.                   | 3                              |
| SA Error                         | 3105               | Indicates a Security Association (SA) error message.               | 5                              |
| SA Creation Failure              | 3106               | Indicates a Security Association (SA) creation failure.            | 3                              |
| SA Established                   | 3107               | Indicates that a Security Association (SA) connection established. | 1                              |
| SA Rejected                      | 3108               | Indicates that a Security Association (SA) connection rejected.    | 3                              |
| Deleting SA                      | 3109               | Indicates the deletion of a Security Association (SA).             | 1                              |



*Table 41. Low-level categories and severity levels for the authentication events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                              | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------|--------------------------------|
| Creating SA                     | 3110               | Indicates the creation of a Security Association (SA).          | 1                              |
| Certificate Mismatch            | 3111               | Indicates a certificate mismatch.                               | 3                              |
| Credentials Mismatch            | 3112               | Indicates a credentials mismatch.                               | 3                              |
| Admin Login Attempt             | 3113               | Indicates an admin login attempt.                               | 2                              |
| User Login Attempt              | 3114               | Indicates a user login attempt.                                 | 2                              |
| User Login Successful           | 3115               | Indicates a successful user login.                              | 1                              |
| User Login Failure              | 3116               | Indicates a failed user login.                                  | 3                              |
| SFTP Login Succeeded            | 3117               | Indicates a successful SSH File Transfer Protocol (SFTP) login. | 1                              |
| SFTP Login Failed               | 3118               | Indicates a failed SSH File Transfer Protocol (SFTP) login.     | 3                              |
| SFTP Logout                     | 3119               | Indicates an SSH File Transfer Protocol (SFTP) logout.          | 1                              |
| Identity Granted                | 3120               | Indicates that an identity was granted.                         | 1                              |
| Identity Removed                | 3121               | Indicates that an identity was removed.                         | 1                              |
| Identity Revoked                | 3122               | Indicates that an identity was revoked.                         | 1                              |
| Policy Removed                  | 3123               | Indicates that a policy was removed.                            | 1                              |
| User Account Lock               | 3124               | Indicates that a user account was locked.                       | 1                              |
| User Account Unlock             | 3125               | Indicates that a user account was unlocked                      | 1                              |
| User Account Expired            | 3126               | Indicates that a user account is expired                        | 1                              |

## Access

The access category contains authentication and access controls that are used for monitoring network events.

The following table describes the low-level event categories and associated severity levels for the access category.

| <i>Table 42. Low-level categories and severity levels for the access events category</i> |                    |                                                                               |                                |
|------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                          | <b>Category ID</b> | <b>Description</b>                                                            | <b>Severity level (0 - 10)</b> |
| Unknown Network Communication Event                                                      | 4001               | Indicates an unknown network communication event.                             | 3                              |
| Firewall Permit                                                                          | 4002               | Indicates that access to the firewall was allowed.                            | 0                              |
| Firewall Deny                                                                            | 4003               | Indicates that access to the firewall was denied.                             | 4                              |
| Flow Context Response (QRadar SIEM only)                                                 | 4004               | Indicates events from the Classification Engine in response to a SIM request. | 5                              |
| Misc Network Communication Event                                                         | 4005               | Indicates a miscellaneous communications event.                               | 3                              |
| IPS Deny                                                                                 | 4006               | Indicates Intrusion Prevention Systems (IPS) denied traffic.                  | 4                              |
| Firewall Session Opened                                                                  | 4007               | Indicates that the firewall session was opened.                               | 0                              |
| Firewall Session Closed                                                                  | 4008               | Indicates that the firewall session was closed.                               | 0                              |
| Dynamic Address Translation Successful                                                   | 4009               | Indicates that dynamic address translation was successful.                    | 0                              |
| No Translation Group Found                                                               | 4010               | Indicates that no translation group was found.                                | 2                              |
| Misc Authorization                                                                       | 4011               | Indicates that access was granted to a miscellaneous authentication server.   | 2                              |
| ACL Permit                                                                               | 4012               | Indicates that an Access Control List (ACL) allowed access.                   | 0                              |
| ACL Deny                                                                                 | 4013               | Indicates that an Access Control List (ACL) denied access.                    | 4                              |

*Table 42. Low-level categories and severity levels for the access events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                          | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------------|--------------------------------|
| Access Permitted                | 4014               | Indicates that access was allowed.                          | 0                              |
| Access Denied                   | 4015               | Indicates that access was denied.                           | 4                              |
| Session Opened                  | 4016               | Indicates that a session was opened.                        | 1                              |
| Session Closed                  | 4017               | Indicates that a session was closed.                        | 1                              |
| Session Reset                   | 4018               | Indicates that a session was reset.                         | 3                              |
| Session Terminated              | 4019               | Indicates that a session was allowed.                       | 4                              |
| Session Denied                  | 4020               | Indicates that a session was denied.                        | 5                              |
| Session in Progress             | 4021               | Indicates that a session is in progress.                    | 1                              |
| Session Delayed                 | 4022               | Indicates that a session was delayed.                       | 3                              |
| Session Queued                  | 4023               | Indicates that a session was queued.                        | 1                              |
| Session Inbound                 | 4024               | Indicates that a session is inbound.                        | 1                              |
| Session Outbound                | 4025               | Indicates that a session is outbound.                       | 1                              |
| Unauthorized Access Attempt     | 4026               | Indicates that an unauthorized access attempt was detected. | 6                              |
| Misc Application Action Allowed | 4027               | Indicates that an application action was allowed.           | 1                              |
| Misc Application Action Denied  | 4028               | Indicates that an application action was denied.            | 3                              |
| Database Action Allowed         | 4029               | Indicates that a database action was allowed.               | 1                              |
| Database Action Denied          | 4030               | Indicates that a database action was denied.                | 3                              |
| FTP Action Allowed              | 4031               | Indicates that an FTP action was allowed.                   | 1                              |

Table 42. Low-level categories and severity levels for the access events category (continued)

| Low-level event category | Category ID | Description                                             | Severity level (0 - 10) |
|--------------------------|-------------|---------------------------------------------------------|-------------------------|
| FTP Action Denied        | 4032        | Indicates that an FTP action was denied.                | 3                       |
| Object Cached            | 4033        | Indicates that an object was cached.                    | 1                       |
| Object Not Cached        | 4034        | Indicates that an object was not cached.                | 1                       |
| Rate Limiting            | 4035        | Indicates that the network rate-limits traffic.         | 4                       |
| No Rate Limiting         | 4036        | Indicates that the network does not rate-limit traffic. | 0                       |
| P11 Access Permitted     | 4037        | Indicates that P11 access is permitted.                 | 8                       |
| P11 Access Denied        | 4038        | Indicates that P11 access was attempted and denied.     | 8                       |
| IPS Permit               | 4039        | Indicates an IPS permit.                                | 0                       |

## Exploit

The exploit category contains events where a communication or an access exploit occurred.

The following table describes the low-level event categories and associated severity levels for the exploit category.

Table 43. Low-level categories and severity levels for the exploit events category

| Low-level event category | Category ID | Description                            | Severity level (0 - 10) |
|--------------------------|-------------|----------------------------------------|-------------------------|
| Unknown Exploit Attack   | 5001        | Indicates an unknown exploit attack.   | 9                       |
| Buffer Overflow          | 5002        | Indicates a buffer overflow.           | 9                       |
| DNS Exploit              | 5003        | Indicates a DNS exploit.               | 9                       |
| Telnet Exploit           | 5004        | Indicates a Telnet exploit.            | 9                       |
| Linux Exploit            | 5005        | Indicates a Linux exploit.             | 9                       |
| UNIX Exploit             | 5006        | Indicates a UNIX exploit.              | 9                       |
| Windows Exploit          | 5007        | Indicates a Microsoft Windows exploit. | 9                       |
| Mail Exploit             | 5008        | Indicates a mail server exploit.       | 9                       |

Table 43. Low-level categories and severity levels for the exploit events category (continued)

| Low-level event category    | Category ID | Description                                                                             | Severity level (0 - 10) |
|-----------------------------|-------------|-----------------------------------------------------------------------------------------|-------------------------|
| Infrastructure Exploit      | 5009        | Indicates an infrastructure exploit.                                                    | 9                       |
| Misc Exploit                | 5010        | Indicates a miscellaneous exploit.                                                      | 9                       |
| Web Exploit                 | 5011        | Indicates a web exploit.                                                                | 9                       |
| Session Hijack              | 5012        | Indicates that a session in your network was interceded.                                | 9                       |
| Worm Active                 | 5013        | Indicates an active worm.                                                               | 10                      |
| Password Guess/<br>Retrieve | 5014        | Indicates that a user requested access to their password information from the database. | 9                       |
| FTP Exploit                 | 5015        | Indicates an FTP exploit.                                                               | 9                       |
| RPC Exploit                 | 5016        | Indicates an RPC exploit.                                                               | 9                       |
| SNMP Exploit                | 5017        | Indicates an SNMP exploit.                                                              | 9                       |
| NOOP Exploit                | 5018        | Indicates an NOOP exploit.                                                              | 9                       |
| Samba Exploit               | 5019        | Indicates a Samba exploit.                                                              | 9                       |
| SSH Exploit                 | 5020        | Indicates an SSH exploit.                                                               | 9                       |
| Database Exploit            | 5021        | Indicates a database exploit.                                                           | 9                       |
| ICMP Exploit                | 5022        | Indicates an ICMP exploit.                                                              | 9                       |
| UDP Exploit                 | 5023        | Indicates a UDP exploit.                                                                | 9                       |
| Browser Exploit             | 5024        | Indicates an exploit on your browser.                                                   | 9                       |
| DHCP Exploit                | 5025        | Indicates a DHCP exploit                                                                | 9                       |
| Remote Access Exploit       | 5026        | Indicates a remote access exploit                                                       | 9                       |
| ActiveX Exploit             | 5027        | Indicates an exploit through an ActiveX application.                                    | 9                       |
| SQL Injection               | 5028        | Indicates that an SQL injection occurred.                                               | 9                       |

*Table 43. Low-level categories and severity levels for the exploit events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                               | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------------|--------------------------------|
| Cross-Site Scripting            | 5029               | Indicates a cross-site scripting vulnerability.                  | 9                              |
| Format String Vulnerability     | 5030               | Indicates a format string vulnerability.                         | 9                              |
| Input Validation Exploit        | 5031               | Indicates that an input validation exploit attempt was detected. | 9                              |
| Remote Code Execution           | 5032               | Indicates that a remote code execution attempt was detected.     | 9                              |
| Memory Corruption               | 5033               | Indicates that a memory corruption exploit was detected.         | 9                              |
| Command Execution               | 5034               | Indicates that a remote command execution attempt was detected.  | 9                              |
| Code Injection                  | 5035               | Indicates that a code injection was detected.                    | 9                              |
| Replay Attack                   | 5036               | Indicates that a replay attack was detected.                     | 9                              |

## Malware

The malicious software (malware) category contains events that are related to application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the malware category.

*Table 44. Low-level categories and severity levels for the malware events category*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                     | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------|--------------------------------|
| Unknown Malware                 | 6001               | Indicates an unknown virus.                            | 4                              |
| Backdoor Detected               | 6002               | Indicates that a back door to the system was detected. | 9                              |
| Hostile Mail Attachment         | 6003               | Indicates a hostile mail attachment.                   | 6                              |
| Malicious Software              | 6004               | Indicates a virus.                                     | 6                              |
| Hostile Software Download       | 6005               | Indicates a hostile software download to your network. | 6                              |
| Virus Detected                  | 6006               | Indicates that a virus was detected.                   | 8                              |

Table 44. Low-level categories and severity levels for the malware events category (continued)

| Low-level event category | Category ID | Description                                                    | Severity level (0 - 10) |
|--------------------------|-------------|----------------------------------------------------------------|-------------------------|
| Misc Malware             | 6007        | Indicates miscellaneous malicious software                     | 4                       |
| Trojan Detected          | 6008        | Indicates that a trojan was detected.                          | 7                       |
| Spyware Detected         | 6009        | Indicates that spyware was detected on your system.            | 6                       |
| Content Scan             | 6010        | Indicates that an attempted scan of your content was detected. | 3                       |
| Content Scan Failed      | 6011        | Indicates that a scan of your content failed.                  | 8                       |
| Content Scan Successful  | 6012        | Indicates that a scan of your content was successful.          | 3                       |
| Content Scan in Progress | 6013        | Indicates that a scan of your content is in progress.          | 3                       |
| Keylogger                | 6014        | Indicates that a key logger was detected.                      | 7                       |
| Adware Detected          | 6015        | Indicates that Ad-Ware was detected.                           | 4                       |
| Quarantine Successful    | 6016        | Indicates that a quarantine action successfully completed.     | 3                       |
| Quarantine Failed        | 6017        | Indicates that a quarantine action failed.                     | 8                       |
| Malware Infection        | 6018        | Indicates that a malware infection was detected.               | 10                      |
| Remove Successful        | 6019        | Indicates that the removal was successful.                     | 3                       |
| Remove Failed            | 6020        | Indicates that the removal failed.                             | 8                       |

## Suspicious Activity

The suspicious category contains events that are related to viruses, trojans, back door attacks, and other forms of hostile software.

The following table describes the low-level event categories and associated severity levels for the suspicious activity category.

*Table 45. Low-level categories and severity levels for the suspicious activity events category*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                   | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------|--------------------------------|
| Unknown Suspicious Event        | 7001               | Indicates an unknown suspicious event.               | 3                              |
| Suspicious Pattern Detected     | 7002               | Indicates that a suspicious pattern was detected.    | 3                              |
| Content Modified By Firewall    | 7003               | Indicates that content was modified by the firewall. | 3                              |
| Invalid Command or Data         | 7004               | Indicates an invalid command or data.                | 3                              |
| Suspicious Packet               | 7005               | Indicates a suspicious packet.                       | 3                              |
| Suspicious Activity             | 7006               | Indicates suspicious activity.                       | 3                              |
| Suspicious File Name            | 7007               | Indicates a suspicious file name.                    | 3                              |
| Suspicious Port Activity        | 7008               | Indicates suspicious port activity.                  | 3                              |
| Suspicious Routing              | 7009               | Indicates suspicious routing.                        | 3                              |
| Potential Web Vulnerability     | 7010               | Indicates potential web vulnerability.               | 3                              |
| Unknown Evasion Event           | 7011               | Indicates an unknown evasion event.                  | 5                              |
| IP Spoof                        | 7012               | Indicates an IP spoof.                               | 5                              |
| IP Fragmentation                | 7013               | Indicates IP fragmentation.                          | 3                              |
| Overlapping IP Fragments        | 7014               | Indicates overlapping IP fragments.                  | 5                              |
| IDS Evasion                     | 7015               | Indicates an IDS evasion.                            | 5                              |
| DNS Protocol Anomaly            | 7016               | Indicates a DNS protocol anomaly.                    | 3                              |
| FTP Protocol Anomaly            | 7017               | Indicates an FTP protocol anomaly.                   | 3                              |
| Mail Protocol Anomaly           | 7018               | Indicates a mail protocol anomaly.                   | 3                              |
| Routing Protocol Anomaly        | 7019               | Indicates a routing protocol anomaly.                | 3                              |
| Web Protocol Anomaly            | 7020               | Indicates a web protocol anomaly.                    | 3                              |



*Table 45. Low-level categories and severity levels for the suspicious activity events category (continued)*

| <b>Low-level event category</b>  | <b>Category ID</b> | <b>Description</b>                                             | <b>Severity level (0 - 10)</b> |
|----------------------------------|--------------------|----------------------------------------------------------------|--------------------------------|
| SQL Protocol Anomaly             | 7021               | Indicates an SQL protocol anomaly.                             | 3                              |
| Executable Code Detected         | 7022               | Indicates that an executable code was detected.                | 5                              |
| Misc Suspicious Event            | 7023               | Indicates a miscellaneous suspicious event.                    | 3                              |
| Information Leak                 | 7024               | Indicates an information leak.                                 | 1                              |
| Potential Mail Vulnerability     | 7025               | Indicates a potential vulnerability in the mail server.        | 4                              |
| Potential Version Vulnerability  | 7026               | Indicates a potential vulnerability in the IBM QRadar version. | 4                              |
| Potential FTP Vulnerability      | 7027               | Indicates a potential FTP vulnerability.                       | 4                              |
| Potential SSH Vulnerability      | 7028               | Indicates a potential SSH vulnerability.                       | 4                              |
| Potential DNS Vulnerability      | 7029               | Indicates a potential vulnerability in the DNS server.         | 4                              |
| Potential SMB Vulnerability      | 7030               | Indicates a potential SMB (Samba) vulnerability.               | 4                              |
| Potential Database Vulnerability | 7031               | Indicates a potential vulnerability in the database.           | 4                              |
| IP Protocol Anomaly              | 7032               | Indicates a potential IP protocol anomaly                      | 3                              |
| Suspicious IP Address            | 7033               | Indicates that a suspicious IP address was detected.           | 2                              |
| Invalid IP Protocol Usage        | 7034               | Indicates an invalid IP protocol.                              | 2                              |
| Invalid Protocol                 | 7035               | Indicates an invalid protocol.                                 | 4                              |
| Suspicious Window Events         | 7036               | Indicates a suspicious event with a screen on your desktop.    | 2                              |
| Suspicious ICMP Activity         | 7037               | Indicates suspicious ICMP activity.                            | 2                              |

*Table 45. Low-level categories and severity levels for the suspicious activity events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                          | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------------------|--------------------------------|
| Potential NFS Vulnerability     | 7038               | Indicates a potential network file system (NFS) vulnerability.              | 4                              |
| Potential NNTP Vulnerability    | 7039               | Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.  | 4                              |
| Potential RPC Vulnerability     | 7040               | Indicates a potential RPC vulnerability.                                    | 4                              |
| Potential Telnet Vulnerability  | 7041               | Indicates a potential Telnet vulnerability on your system.                  | 4                              |
| Potential SNMP Vulnerability    | 7042               | Indicates a potential SNMP vulnerability.                                   | 4                              |
| Illegal TCP Flag Combination    | 7043               | Indicates that an invalid TCP flag combination was detected.                | 5                              |
| Suspicious TCP Flag Combination | 7044               | Indicates that a potentially invalid TCP flag combination was detected.     | 4                              |
| Illegal ICMP Protocol Usage     | 7045               | Indicates that an invalid use of the ICMP protocol was detected.            | 5                              |
| Suspicious ICMP Protocol Usage  | 7046               | Indicates that a potentially invalid use of the ICMP protocol was detected. | 4                              |
| Illegal ICMP Type               | 7047               | Indicates that an invalid ICMP type was detected.                           | 5                              |
| Illegal ICMP Code               | 7048               | Indicates that an invalid ICMP code was detected.                           | 5                              |
| Suspicious ICMP Type            | 7049               | Indicates that a potentially invalid ICMP type was detected.                | 4                              |
| Suspicious ICMP Code            | 7050               | Indicates that a potentially invalid ICMP code was detected.                | 4                              |
| TCP port 0                      | 7051               | Indicates a TCP packet uses a reserved port (0) for source or destination.  | 4                              |

*Table 45. Low-level categories and severity levels for the suspicious activity events category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                            | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------------------------------|--------------------------------|
| UDP port 0                      | 7052               | Indicates a UDP packet uses a reserved port (0) for source or destination.    | 4                              |
| Hostile IP                      | 7053               | Indicates the use of a known hostile IP address.                              | 4                              |
| Watch list IP                   | 7054               | Indicates the use of an IP address from a watch list of IP addresses.         | 4                              |
| Known offender IP               | 7055               | Indicates the use of an IP address of a known offender.                       | 4                              |
| RFC 1918 (private) IP           | 7056               | Indicates the use of an IP address from a private IP address range.           | 4                              |
| Potential VoIP Vulnerability    | 7057               | Indicates a potential VoIP vulnerability.                                     | 4                              |
| Blacklist Address               | 7058               | Indicates that an IP address is on the black list.                            | 8                              |
| Watchlist Address               | 7059               | Indicates that the IP address is on the list of IP addresses being monitored. | 7                              |
| Darknet Address                 | 7060               | Indicates that the IP address is part of a darknet.                           | 5                              |
| Botnet Address                  | 7061               | Indicates that the address is part of a botnet.                               | 7                              |
| Suspicious Address              | 7062               | Indicates that the IP address must be monitored.                              | 5                              |
| Bad Content                     | 7063               | Indicates that bad content was detected.                                      | 7                              |
| Invalid Cert                    | 7064               | Indicates that an invalid certificate was detected.                           | 7                              |
| User Activity                   | 7065               | Indicates that user activity was detected.                                    | 7                              |
| Suspicious Protocol Usage       | 7066               | Indicates that suspicious protocol usage was detected.                        | 5                              |

Table 45. Low-level categories and severity levels for the suspicious activity events category (continued)

| Low-level event category  | Category ID | Description                                                                 | Severity level (0 - 10) |
|---------------------------|-------------|-----------------------------------------------------------------------------|-------------------------|
| Suspicious BGP Activity   | 7067        | Indicates that suspicious Border Gateway Protocol (BGP) usage was detected. | 5                       |
| Route Poisoning           | 7068        | Indicates that route corruption was detected.                               | 5                       |
| ARP Poisoning             | 7069        | Indicates that ARP-cache poisoning was detected.                            | 5                       |
| Rogue Device Detected     | 7070        | Indicates that a rogue device was detected.                                 | 5                       |
| Government Agency Address | 7071        | Indicates that a government agency address was detected.                    | 3                       |

## System

The system category contains events that are related to system changes, software installation, or status messages.

The following table describes the low-level event categories and associated severity levels for the system category.

Table 46. Low-level categories and severity levels for the system events category

| Low-level event category | Category ID | Description                                     | Severity level (0 - 10) |
|--------------------------|-------------|-------------------------------------------------|-------------------------|
| Unknown System Event     | 8001        | Indicates an unknown system event.              | 1                       |
| System Boot              | 8002        | Indicates a system restart.                     | 1                       |
| System Configuration     | 8003        | Indicates a change in the system configuration. | 1                       |
| System Halt              | 8004        | Indicates that the system was halted.           | 1                       |
| System Failure           | 8005        | Indicates a system failure.                     | 6                       |
| System Status            | 8006        | Indicates any information event.                | 1                       |
| System Error             | 8007        | Indicates a system error.                       | 3                       |
| Misc System Event        | 8008        | Indicates a miscellaneous system event.         | 1                       |

Table 46. Low-level categories and severity levels for the system events category (continued)

| Low-level event category              | Category ID | Description                                                        | Severity level (0 - 10) |
|---------------------------------------|-------------|--------------------------------------------------------------------|-------------------------|
| Service Started                       | 8009        | Indicates that system services started.                            | 1                       |
| Service Stopped                       | 8010        | Indicates that system services stopped.                            | 1                       |
| Service Failure                       | 8011        | Indicates a system failure.                                        | 6                       |
| Successful Registry Modification      | 8012        | Indicates that a modification to the registry was successful.      | 1                       |
| Successful Host-Policy Modification   | 8013        | Indicates that a modification to the host policy was successful.   | 1                       |
| Successful File Modification          | 8014        | Indicates that a modification to a file was successful.            | 1                       |
| Successful Stack Modification         | 8015        | Indicates that a modification to the stack was successful.         | 1                       |
| Successful Application Modification   | 8016        | Indicates that a modification to the application was successful.   | 1                       |
| Successful Configuration Modification | 8017        | Indicates that a modification to the configuration was successful. | 1                       |
| Successful Service Modification       | 8018        | Indicates that a modification to a service was successful.         | 1                       |
| Failed Registry Modification          | 8019        | Indicates that a modification to the registry failed.              | 1                       |
| Failed Host-Policy Modification       | 8020        | Indicates that a modification to the host policy failed.           | 1                       |
| Failed File Modification              | 8021        | Indicates that a modification to a file failed.                    | 1                       |
| Failed Stack Modification             | 8022        | Indicates that a modification to the stack failed.                 | 1                       |
| Failed Application Modification       | 8023        | Indicates that a modification to an application failed.            | 1                       |

Table 46. Low-level categories and severity levels for the system events category (continued)

| Low-level event category          | Category ID | Description                                                      | Severity level (0 - 10) |
|-----------------------------------|-------------|------------------------------------------------------------------|-------------------------|
| Failed Configuration Modification | 8024        | Indicates that a modification to the configuration failed.       | 1                       |
| Failed Service Modification       | 8025        | Indicates that a modification to the service failed.             | 1                       |
| Registry Addition                 | 8026        | Indicates that a new item was added to the registry.             | 1                       |
| Host-Policy Created               | 8027        | Indicates that a new entry was added to the registry.            | 1                       |
| File Created                      | 8028        | Indicates that a new was created in the system.                  | 1                       |
| Application Installed             | 8029        | Indicates that a new application was installed on the system.    | 1                       |
| Service Installed                 | 8030        | Indicates that a new service was installed on the system.        | 1                       |
| Registry Deletion                 | 8031        | Indicates that a registry entry was deleted.                     | 1                       |
| Host-Policy Deleted               | 8032        | Indicates that a host policy entry was deleted.                  | 1                       |
| File Deleted                      | 8033        | Indicates that a file was deleted.                               | 1                       |
| Application Uninstalled           | 8034        | Indicates that an application was uninstalled.                   | 1                       |
| Service Uninstalled               | 8035        | Indicates that a service was uninstalled.                        | 1                       |
| System Informational              | 8036        | Indicates system information.                                    | 3                       |
| System Action Allow               | 8037        | Indicates that an attempted action on the system was authorized. | 3                       |
| System Action Deny                | 8038        | Indicates that an attempted action on the system was denied.     | 4                       |
| Cron                              | 8039        | Indicates a crontab message.                                     | 1                       |

Table 46. Low-level categories and severity levels for the system events category (continued)

| Low-level event category | Category ID | Description                                    | Severity level (0 - 10) |
|--------------------------|-------------|------------------------------------------------|-------------------------|
| Cron Status              | 8040        | Indicates a crontab status message.            | 1                       |
| Cron Failed              | 8041        | Indicates a crontab failure message.           | 4                       |
| Cron Successful          | 8042        | Indicates a crontab success message.           | 1                       |
| Daemon                   | 8043        | Indicates a daemon message.                    | 1                       |
| Daemon Status            | 8044        | Indicates a daemon status message.             | 1                       |
| Daemon Failed            | 8045        | Indicates a daemon failure message.            | 4                       |
| Daemon Successful        | 8046        | Indicates a daemon success message.            | 1                       |
| Kernel                   | 8047        | Indicates a kernel message.                    | 1                       |
| Kernel Status            | 8048        | Indicates a kernel status message.             | 1                       |
| Kernel Failed            | 8049        | Indicates a kernel failure message.            |                         |
| Kernel Successful        | 8050        | Indicates a kernel successful message.         | 1                       |
| Authentication           | 8051        | Indicates an authentication message.           | 1                       |
| Information              | 8052        | Indicates an informational message.            | 2                       |
| Notice                   | 8053        | Indicates a notice message.                    | 3                       |
| Warning                  | 8054        | Indicates a warning message.                   | 5                       |
| Error                    | 8055        | Indicates an error message.                    | 7                       |
| Critical                 | 8056        | Indicates a critical message.                  | 9                       |
| Debug                    | 8057        | Indicates a debug message.                     | 1                       |
| Messages                 | 8058        | Indicates a generic message.                   | 1                       |
| Privilege Access         | 8059        | Indicates that privilege access was attempted. | 3                       |

Table 46. Low-level categories and severity levels for the system events category (continued)

| Low-level event category                             | Category ID | Description                                                                          | Severity level (0 - 10) |
|------------------------------------------------------|-------------|--------------------------------------------------------------------------------------|-------------------------|
| Alert                                                | 8060        | Indicates an alert message.                                                          | 9                       |
| Emergency                                            | 8061        | Indicates an emergency message.                                                      | 9                       |
| SNMP Status                                          | 8062        | Indicates an SNMP status message.                                                    | 1                       |
| FTP Status                                           | 8063        | Indicates an FTP status message.                                                     | 1                       |
| NTP Status                                           | 8064        | Indicates an NTP status message.                                                     | 1                       |
| Access Point Radio Failure                           | 8065        | Indicates an access point radio failure.                                             | 3                       |
| Encryption Protocol Configuration Mismatch           | 8066        | Indicates an encryption protocol configuration mismatch.                             | 3                       |
| Client Device or Authentication Server Misconfigured | 8067        | Indicates that a client device or authentication server was not configured properly. | 5                       |
| Hot Standby Enable Failed                            | 8068        | Indicates a hot standby enable failure.                                              | 5                       |
| Hot Standby Disable Failed                           | 8069        | Indicates a hot standby disable failure.                                             | 5                       |
| Hot Standby Enabled Successfully                     | 8070        | Indicates that hot standby was enabled successfully.                                 | 1                       |
| Hot Standby Association Lost                         | 8071        | Indicates that a hot standby association was lost.                                   | 5                       |
| MainMode Initiation Failure                          | 8072        | Indicates MainMode initiation failure.                                               | 5                       |
| MainMode Initiation Succeeded                        | 8073        | Indicates that the MainMode initiation was successful.                               | 1                       |
| MainMode Status                                      | 8074        | Indicates a MainMode status message was reported.                                    | 1                       |
| QuickMode Initiation Failure                         | 8075        | Indicates that the QuickMode initiation failed.                                      | 5                       |
| Quickmode Initiation Succeeded                       | 8076        | Indicates that the QuickMode initiation was successful.                              | 1                       |



| <i>Table 46. Low-level categories and severity levels for the system events category (continued)</i> |                    |                                                                           |                                |
|------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                      | <b>Category ID</b> | <b>Description</b>                                                        | <b>Severity level (0 - 10)</b> |
| Quickmode Status                                                                                     | 8077               | Indicates a QuickMode status message was reported.                        | 1                              |
| Invalid License                                                                                      | 8078               | Indicates an invalid license.                                             | 3                              |
| License Expired                                                                                      | 8079               | Indicates an expired license.                                             | 3                              |
| New License Applied                                                                                  | 8080               | Indicates a new license applied.                                          | 1                              |
| License Error                                                                                        | 8081               | Indicates a license error.                                                | 5                              |
| License Status                                                                                       | 8082               | Indicates a license status message.                                       | 1                              |
| Configuration Error                                                                                  | 8083               | Indicates that a configuration error was detected.                        | 5                              |
| Service Disruption                                                                                   | 8084               | Indicates that a service disruption was detected.                         | 5                              |
| EPS or FPM allocation exceeded                                                                       | 8085               | Indicates that the license pool allocations for EPS or FPM were exceeded. | 3                              |
| Performance Status                                                                                   | 8086               | Indicates that the performance status was reported.                       | 1                              |
| Performance Degradation                                                                              | 8087               | Indicates that the performance is being degraded.                         | 4                              |
| Misconfiguration                                                                                     | 8088               | Indicates that an incorrect configuration was detected.                   | 5                              |

## Policy

The policy category contains events that are related to administration of network policy and the monitoring network resources for policy violations.

The following table describes the low-level event categories and associated severity levels for the policy category.

| <i>Table 47. Low-level categories and severity levels for the policy category</i> |                    |                                        |                                |
|-----------------------------------------------------------------------------------|--------------------|----------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                   | <b>Category ID</b> | <b>Description</b>                     | <b>Severity level (0 - 10)</b> |
| Unknown Policy Violation                                                          | 9001               | Indicates an unknown policy violation. | 2                              |

Table 47. Low-level categories and severity levels for the policy category (continued)

| Low-level event category           | Category ID | Description                                                                      | Severity level (0 - 10) |
|------------------------------------|-------------|----------------------------------------------------------------------------------|-------------------------|
| Web Policy Violation               | 9002        | Indicates a web policy violation.                                                | 2                       |
| Remote Access Policy Violation     | 9003        | Indicates a remote access policy violation.                                      | 2                       |
| IRC/IM Policy Violation            | 9004        | Indicates an instant messenger policy violation.                                 | 2                       |
| P2P Policy Violation               | 9005        | Indicates a Peer-to-Peer (P2P) policy violation.                                 | 2                       |
| IP Access Policy Violation         | 9006        | Indicates an IP access policy violation.                                         | 2                       |
| Application Policy Violation       | 9007        | Indicates an application policy violation.                                       | 2                       |
| Database Policy Violation          | 9008        | Indicates a database policy violation.                                           | 2                       |
| Network Threshold Policy Violation | 9009        | Indicates a network threshold policy violation.                                  | 2                       |
| Porn Policy Violation              | 9010        | Indicates a porn policy violation.                                               | 2                       |
| Games Policy Violation             | 9011        | Indicates a games policy violation.                                              | 2                       |
| Misc Policy Violation              | 9012        | Indicates a miscellaneous policy violation.                                      | 2                       |
| Compliance Policy Violation        | 9013        | Indicates a compliance policy violation.                                         | 2                       |
| Mail Policy Violation              | 9014        | Indicates a mail policy violation.                                               | 2                       |
| IRC Policy Violation               | 9015        | Indicates an IRC policy violation                                                | 2                       |
| IM Policy Violation                | 9016        | Indicates a policy violation that is related to instant message (IM) activities. | 2                       |
| VoIP Policy Violation              | 9017        | Indicates a VoIP policy violation                                                | 2                       |
| Succeeded                          | 9018        | Indicates a policy successful message.                                           | 1                       |
| Failed                             | 9019        | Indicates a policy failure message.                                              | 4                       |

| <i>Table 47. Low-level categories and severity levels for the policy category (continued)</i> |                    |                                                    |                                |
|-----------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                               | <b>Category ID</b> | <b>Description</b>                                 | <b>Severity level (0 - 10)</b> |
| Data Loss Prevention Policy Violation                                                         | 9020               | Indicates a data loss prevention policy violation. | 2                              |
| Watchlist Object                                                                              | 9021               | Indicates a watchlist object.                      | 2                              |
| Web Policy Allow                                                                              | 9022               | Indicates a new web policy allowance.              | 1                              |

## Unknown

The Unknown category contains events that are not parsed and therefore cannot be categorized.

The following table describes the low-level event categories and associated severity levels for the Unknown category.

| <i>Table 48. Low-level categories and severity levels for the Unknown category</i> |                    |                                                                            |                                |
|------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                    | <b>Category ID</b> | <b>Description</b>                                                         | <b>Severity level (0 - 10)</b> |
| Unknown                                                                            | 10001              | Indicates an unknown event.                                                | 3                              |
| Unknown Snort Event                                                                | 10002              | Indicates an unknown Snort event.                                          | 3                              |
| Unknown Dragon Event                                                               | 10003              | Indicates an unknown Dragon event.                                         | 3                              |
| Unknown Pix Firewall Event                                                         | 10004              | Indicates an unknown Cisco Private Internet Exchange (PIX) Firewall event. | 3                              |
| Unknown Tipping Point Event                                                        | 10005              | Indicates an unknown HP TippingPoint event.                                | 3                              |
| Unknown Windows Auth Server Event                                                  | 10006              | Indicates an unknown Windows Auth Server event.                            | 3                              |
| Unknown Nortel Event                                                               | 10007              | Indicates an unknown Nortel event.                                         | 3                              |
| Stored                                                                             | 10009              | Indicates an unknown stored event.                                         | 3                              |
| Behavioral                                                                         | 11001              | Indicates an unknown behavioral event.                                     | 3                              |
| Threshold                                                                          | 11002              | Indicates an unknown threshold event.                                      | 3                              |
| Anomaly                                                                            | 11003              | Indicates an unknown anomaly event.                                        | 3                              |

## CRE

The custom rule event (CRE) category contains events that are generated from a custom offense, flow, or event rule.

The following table describes the low-level event categories and associated severity levels for the CRE category.

| <i>Table 49. Low-level categories and severity levels for the CRE category</i> |                    |                                                      |                                |
|--------------------------------------------------------------------------------|--------------------|------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                | <b>Category ID</b> | <b>Description</b>                                   | <b>Severity level (0 - 10)</b> |
| Unknown CRE Event                                                              | 12001              | Indicates an unknown custom rules engine event.      | 5                              |
| Single Event Rule Match                                                        | 12002              | Indicates a single event rule match.                 | 5                              |
| Event Sequence Rule Match                                                      | 12003              | Indicates an event sequence rule match.              | 5                              |
| Cross-Offense Event Sequence Rule Match                                        | 12004              | Indicates a cross-offense event sequence rule match. | 5                              |
| Offense Rule Match                                                             | 12005              | Indicates an offense rule match.                     | 5                              |

## Potential Exploit

The potential exploit category contains events that are related to potential application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the potential exploit category.

| <i>Table 50. Low-level categories and severity levels for the potential exploit category</i> |                    |                                                                                       |                                |
|----------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                              | <b>Category ID</b> | <b>Description</b>                                                                    | <b>Severity level (0 - 10)</b> |
| Unknown Potential Exploit Attack                                                             | 13001              | Indicates that a potential exploitative attack was detected.                          | 7                              |
| Potential Buffer Overflow                                                                    | 13002              | Indicates that a potential buffer overflow was detected.                              | 7                              |
| Potential DNS Exploit                                                                        | 13003              | Indicates that a potentially exploitative attack through the DNS server was detected. | 7                              |
| Potential Telnet Exploit                                                                     | 13004              | Indicates that a potentially exploitative attack through Telnet was detected.         | 7                              |

Table 50. Low-level categories and severity levels for the potential exploit category (continued)

| Low-level event category         | Category ID | Description                                                                               | Severity level (0 - 10) |
|----------------------------------|-------------|-------------------------------------------------------------------------------------------|-------------------------|
| Potential Linux Exploit          | 13005       | Indicates that a potentially exploitative attack through Linux was detected.              | 7                       |
| Potential UNIX Exploit           | 13006       | Indicates that a potentially exploitative attack through UNIX was detected.               | 7                       |
| Potential Windows Exploit        | 13007       | Indicates that a potentially exploitative attack through Windows was detected.            | 7                       |
| Potential Mail Exploit           | 13008       | Indicates that a potentially exploitative attack through mail was detected.               | 7                       |
| Potential Infrastructure Exploit | 13009       | Indicates that a potential exploitative attack on the system infrastructure was detected. | 7                       |
| Potential Misc Exploit           | 13010       | Indicates that a potentially exploitative attack was detected.                            | 7                       |
| Potential Web Exploit            | 13011       | Indicates that a potentially exploitative attack through the web was detected.            | 7                       |
| Potential Botnet Connection      | 13012       | Indicates a potentially exploitative attack that uses botnet was detected.                | 6                       |
| Potential Worm Activity          | 13013       | Indicates a potential attack that uses worm activity was detected.                        | 6                       |

## Flow

The flow category includes events that are related to flow actions.

The following table describes the low-level event categories and associated severity levels for the flow category.

*Table 51. Low-level categories and severity levels for the flow category*

| <b>Low-level event category</b>            | <b>Category ID</b> | <b>Description</b>                                           | <b>Severity level (0 - 10)</b> |
|--------------------------------------------|--------------------|--------------------------------------------------------------|--------------------------------|
| Unidirectional Flow                        | 14001              | Indicates a unidirectional flow of events.                   | 5                              |
| Low number of Unidirectional Flows         | 14002              | Indicates a low number of unidirectional flows of events.    | 5                              |
| Medium number of Unidirectional Flows      | 14003              | Indicates a medium number of unidirectional flows of events. | 5                              |
| High number of Unidirectional Flows        | 14004              | Indicates a high number of unidirectional flows of events.   | 5                              |
| Unidirectional TCP Flow                    | 14005              | Indicates a unidirectional TCP flow.                         | 5                              |
| Low number of Unidirectional TCP Flows     | 14006              | Indicates a low number of unidirectional TCP flows.          | 5                              |
| Medium number of Unidirectional TCP Flows  | 14007              | Indicates a medium number of unidirectional TCP flows.       | 5                              |
| High number of Unidirectional TCP Flows    | 14008              | Indicates a high number of unidirectional TCP flows.         | 5                              |
| Unidirectional ICMP Flow                   | 14009              | Indicates a unidirectional ICMP flow.                        | 5                              |
| Low number of Unidirectional ICMP Flows    | 14010              | Indicates a low number of unidirectional ICMP flows.         | 5                              |
| Medium number of Unidirectional ICMP Flows | 14011              | Indicates a medium number of unidirectional ICMP flows.      | 5                              |
| High number if Unidirectional ICMP Flows   | 14012              | Indicates a high number of unidirectional ICMP flows.        | 5                              |
| Suspicious ICMP Flow                       | 14013              | Indicates a suspicious ICMP flow.                            | 5                              |
| Suspicious UDP Flow                        | 14014              | Indicates a suspicious UDP flow.                             | 5                              |
| Suspicious TCP Flow                        | 14015              | Indicates a suspicious TCP flow.                             | 5                              |
| Suspicious Flow                            | 14016              | Indicates a suspicious flow.                                 | 5                              |
| Empty Packet Flows                         | 14017              | Indicates empty packet flows.                                | 5                              |
| Low number of Empty Packet Flows           | 14018              | Indicates a low number of empty packet flows.                | 5                              |
| Medium number of Empty Packet Flows        | 14019              | Indicates a medium number of empty packet flows.             | 5                              |
| High number of Empty Packet Flows          | 14020              | Indicates a high number of empty packet flows.               | 5                              |

| <i>Table 51. Low-level categories and severity levels for the flow category (continued)</i> |                    |                                                       |                                |
|---------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                             | <b>Category ID</b> | <b>Description</b>                                    | <b>Severity level (0 - 10)</b> |
| Large Payload Flows                                                                         | 14021              | Indicates a large payload of flows.                   | 5                              |
| Low number of Large Payload Flows                                                           | 14022              | Indicates a low number of large payload flows.        | 5                              |
| Medium number of Large Payload Flows                                                        | 14023              | Indicates a medium number of large payload flows.     | 5                              |
| High number of Large Payload Flows                                                          | 14024              | Indicates a high number of large payload flows.       | 5                              |
| One Attacker to Many Target Flows                                                           | 14025              | Indicates that one attacker is targeting many flows.  | 5                              |
| Many Attacker to one Target Flow                                                            | 14026              | Indicates that many attackers are targeting one flow. | 5                              |
| Unknown Flow                                                                                | 14027              | Indicates an unknown flow.                            | 5                              |
| Netflow Record                                                                              | 14028              | Indicates a Netflow record.                           | 5                              |
| QFlow Record                                                                                | 14029              | Indicates a QFlow record.                             | 5                              |
| SFlow Record                                                                                | 14030              | Indicates an SFlow record.                            | 5                              |
| Packeteer Record                                                                            | 14031              | Indicates a Packeteer record.                         | 5                              |
| Misc Flow                                                                                   | 14032              | Indicates a misc flow.                                | 5                              |
| Large Data Transfer                                                                         | 14033              | Indicates a large transfer of data.                   | 5                              |
| Large Data Transfer Outbound                                                                | 14034              | Indicates a large transfer of outbound data.          | 5                              |
| VoIP Flows                                                                                  | 14035              | Indicates VoIP Flows.                                 | 5                              |

## User Defined

The User Defined category contains events that are related to user-defined objects

The following table describes the low-level event categories and associated severity levels for the User Defined category.

| <i>Table 52. Low-level categories and severity levels for the User Defined category</i> |                    |                                                   |                                |
|-----------------------------------------------------------------------------------------|--------------------|---------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                         | <b>Category ID</b> | <b>Description</b>                                | <b>Severity level (0 - 10)</b> |
| Custom Sentry Low                                                                       | 15001              | Indicates a low severity custom anomaly event.    | 3                              |
| Custom Sentry Medium                                                                    | 15002              | Indicates a medium severity custom anomaly event. | 5                              |
| Custom Sentry High                                                                      | 15003              | Indicates a high severity custom anomaly event.   | 7                              |

Table 52. Low-level categories and severity levels for the User Defined category (continued)

| Low-level event category | Category ID | Description                                                   | Severity level (0 - 10) |
|--------------------------|-------------|---------------------------------------------------------------|-------------------------|
| Custom Sentry 1          | 15004       | Indicates a custom anomaly event with a severity level of 1.  | 1                       |
| Custom Sentry 2          | 15005       | Indicates a custom anomaly event with a severity level of 2.  | 2                       |
| Custom Sentry 3          | 15006       | Indicates a custom anomaly event with a severity level of 3.  | 3                       |
| Custom Sentry 4          | 15007       | Indicates a custom anomaly event with a severity level of 4.  | 4                       |
| Custom Sentry 5          | 15008       | Indicates a custom anomaly event with a severity level of 5.  | 5                       |
| Custom Sentry 6          | 15009       | Indicates a custom anomaly event with a severity level of 6.  | 6                       |
| Custom Sentry 7          | 15010       | Indicates a custom anomaly event with a severity level of 7.  | 7                       |
| Custom Sentry 8          | 15011       | Indicates a custom anomaly event with a severity level of 8.  | 8                       |
| Custom Sentry 9          | 15012       | Indicates a custom anomaly event with a severity level of 9.  | 9                       |
| Custom Policy Low        | 15013       | Indicates a custom policy event with a low severity level.    | 3                       |
| Custom Policy Medium     | 15014       | Indicates a custom policy event with a medium severity level. | 5                       |
| Custom Policy High       | 15015       | Indicates a custom policy event with a high severity level.   | 7                       |
| Custom Policy 1          | 15016       | Indicates a custom policy event with a severity level of 1.   | 1                       |
| Custom Policy 2          | 15017       | Indicates a custom policy event with a severity level of 2.   | 2                       |
| Custom Policy 3          | 15018       | Indicates a custom policy event with a severity level of 3.   | 3                       |



*Table 52. Low-level categories and severity levels for the User Defined category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                          | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------------|--------------------------------|
| Custom Policy 4                 | 15019              | Indicates a custom policy event with a severity level of 4. | 4                              |
| Custom Policy 5                 | 15020              | Indicates a custom policy event with a severity level of 5. | 5                              |
| Custom Policy 6                 | 15021              | Indicates a custom policy event with a severity level of 6. | 6                              |
| Custom Policy 7                 | 15022              | Indicates a custom policy event with a severity level of 7. | 7                              |
| Custom Policy 8                 | 15023              | Indicates a custom policy event with a severity level of 8. | 8                              |
| Custom Policy 9                 | 15024              | Indicates a custom policy event with a severity level of 9. | 9                              |
| Custom User Low                 | 15025              | Indicates a custom user event with a low severity level.    | 3                              |
| Custom User Medium              | 15026              | Indicates a custom user event with a medium severity level. | 5                              |
| Custom User High                | 15027              | Indicates a custom user event with a high severity level.   | 7                              |
| Custom User 1                   | 15028              | Indicates a custom user event with a severity level of 1.   | 1                              |
| Custom User 2                   | 15029              | Indicates a custom user event with a severity level of 2.   | 2                              |
| Custom User 3                   | 15030              | Indicates a custom user event with a severity level of 3.   | 3                              |
| Custom User 4                   | 15031              | Indicates a custom user event with a severity level of 4.   | 4                              |
| Custom User 5                   | 15032              | Indicates a custom user event with a severity level of 5.   | 5                              |
| Custom User 6                   | 15033              | Indicates a custom user event with a severity level of 6.   | 6                              |

*Table 52. Low-level categories and severity levels for the User Defined category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                        | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------|--------------------------------|
| Custom User 7                   | 15034              | Indicates a custom user event with a severity level of 7. | 7                              |
| Custom User 8                   | 15035              | Indicates a custom user event with a severity level of 8. | 8                              |
| Custom User 9                   | 15036              | Indicates a custom user event with a severity level of 9. | 9                              |

## SIM Audit

The SIM Audit category contains events that are related to user interaction with the IBM QRadar Console and administrative features.

The following table describes the low-level event categories and associated severity levels for the SIM Audit category.

*Table 53. Low-level categories and severity levels for the SIM Audit category*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                                              | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------|
| SIM User Authentication         | 16001              | Indicates a user login or logout on the Console.                                                                | 5                              |
| SIM Configuration Change        | 16002              | Indicates that a user changed the SIM configuration or deployment.                                              | 3                              |
| SIM User Action                 | 16003              | Indicates that a user initiated a process, such as starting a backup or generating a report, in the SIM module. | 3                              |
| Session Created                 | 16004              | Indicates that a user session was created.                                                                      | 3                              |
| Session Destroyed               | 16005              | Indicates that a user session was destroyed.                                                                    | 3                              |
| Admin Session Created           | 16006              | Indicates that an admin session was created.                                                                    |                                |
| Admin Session Destroyed         | 16007              | Indicates that an admin session was destroyed.                                                                  | 3                              |
| Session Authentication Invalid  | 16008              | Indicates an invalid session authentication.                                                                    | 5                              |
| Session Authentication Expired  | 16009              | Indicates that a session authentication expired.                                                                | 3                              |

| <i>Table 53. Low-level categories and severity levels for the SIM Audit category (continued)</i> |                    |                                                                          |                                |
|--------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                  | <b>Category ID</b> | <b>Description</b>                                                       | <b>Severity level (0 - 10)</b> |
| Risk Manager Configuration                                                                       | 16010              | Indicates that a user changed the IBM QRadar Risk Manager configuration. | 3                              |

## VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities that are detected on the network, the VIS component generates events. These events are sent to the Event Collector to be correlated with other security events.

The following table describes the low-level event categories and associated severity levels for the VIS host discovery category.

| <i>Table 54. Low-level categories and severity levels for the VIS host discovery category</i> |                    |                                                                             |                                |
|-----------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                               | <b>Category ID</b> | <b>Description</b>                                                          | <b>Severity level (0 - 10)</b> |
| New Host Discovered                                                                           | 17001              | Indicates that the VIS component detected a new host.                       | 3                              |
| New Port Discovered                                                                           | 17002              | Indicates that the VIS component detected a new open port.                  | 3                              |
| New Vuln Discovered                                                                           | 17003              | Indicates that the VIS component detected a new vulnerability.              | 3                              |
| New OS Discovered                                                                             | 17004              | Indicates that the VIS component detected a new operating system on a host. | 3                              |
| Bulk Host Discovered                                                                          | 17005              | Indicates that the VIS component detected many new hosts in a short period. | 3                              |

## Application

The application category contains events that are related to application activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the application category.

| <i>Table 55. Low-level categories and severity levels for the application category</i> |                    |                                                     |                                |
|----------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                        | <b>Category ID</b> | <b>Description</b>                                  | <b>Severity level (0 - 10)</b> |
| Mail Opened                                                                            | 18001              | Indicates that an email connection was established. | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                     | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------|--------------------------------|
| Mail Closed                     | 18002              | Indicates that an email connection was closed.         | 1                              |
| Mail Reset                      | 18003              | Indicates that an email connection was reset.          | 3                              |
| Mail Terminated                 | 18004              | Indicates that an email connection was terminated.     | 4                              |
| Mail Denied                     | 18005              | Indicates that an email connection was denied.         | 4                              |
| Mail in Progress                | 18006              | Indicates that an email connection is being attempted. | 1                              |
| Mail Delayed                    | 18007              | Indicates that an email connection was delayed.        | 4                              |
| Mail Queued                     | 18008              | Indicates that an email connection was queued.         | 3                              |
| Mail Redirected                 | 18009              | Indicates that an email connection was redirected.     | 1                              |
| FTP Opened                      | 18010              | Indicates that an FTP connection was opened.           | 1                              |
| FTP Closed                      | 18011              | Indicates that an FTP connection was closed.           | 1                              |
| FTP Reset                       | 18012              | Indicates that an FTP connection was reset.            | 3                              |
| FTP Terminated                  | 18013              | Indicates that an FTP connection was terminated.       | 4                              |
| FTP Denied                      | 18014              | Indicates that an FTP connection was denied.           | 4                              |
| FTP In Progress                 | 18015              | Indicates that an FTP connection is in progress.       | 1                              |
| FTP Redirected                  | 18016              | Indicates that an FTP connection was redirected.       | 3                              |
| HTTP Opened                     | 18017              | Indicates that an HTTP connection was established.     | 1                              |
| HTTP Closed                     | 18018              | Indicates that an HTTP connection was closed.          | 1                              |
| HTTP Reset                      | 18019              | Indicates that an HTTP connection was reset.           | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                  | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------|--------------------------------|
| HTTP Terminated                 | 18020              | Indicates that an HTTP connection was terminated.   | 4                              |
| HTTP Denied                     | 18021              | Indicates that an HTTP connection was denied.       | 4                              |
| HTTP In Progress                | 18022              | Indicates that an HTTP connection is in progress.   | 1                              |
| HTTP Delayed                    | 18023              | Indicates that an HTTP connection was delayed.      | 3                              |
| HTTP Queued                     | 18024              | Indicates that an HTTP connection was queued.       | 1                              |
| HTTP Redirected                 | 18025              | Indicates that an HTTP connection was redirected.   | 1                              |
| HTTP Proxy                      | 18026              | Indicates that an HTTP connection is being proxied. | 1                              |
| HTTPS Opened                    | 18027              | Indicates that an HTTPS connection was established. | 1                              |
| HTTPS Closed                    | 18028              | Indicates that an HTTPS connection was closed.      | 1                              |
| HTTPS Reset                     | 18029              | Indicates that an HTTPS connection was reset.       | 3                              |
| HTTPS Terminated                | 18030              | Indicates that an HTTPS connection was terminated.  | 4                              |
| HTTPS Denied                    | 18031              | Indicates that an HTTPS connection was denied.      | 4                              |
| HTTPS In Progress               | 18032              | Indicates that an HTTPS connection is in progress.  | 1                              |
| HTTPS Delayed                   | 18033              | Indicates that an HTTPS connection was delayed.     | 3                              |
| HTTPS Queued                    | 18034              | Indicates that an HTTPS connection was queued.      | 3                              |
| HTTPS Redirected                | 18035              | Indicates that an HTTPS connection was redirected.  | 3                              |
| HTTPS Proxy                     | 18036              | Indicates that an HTTPS connection is proxied.      | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                         | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------|--------------------------------|
| SSH Opened                      | 18037              | Indicates that an SSH connection was established.          | 1                              |
| SSH Closed                      | 18038              | Indicates that an SSH connection was closed.               | 1                              |
| SSH Reset                       | 18039              | Indicates that an SSH connection was reset.                | 3                              |
| SSH Terminated                  | 18040              | Indicates that an SSH connection was terminated.           | 4                              |
| SSH Denied                      | 18041              | Indicates that an SSH session was denied.                  | 4                              |
| SSH In Progress                 | 18042              | Indicates that an SSH session is in progress.              | 1                              |
| RemoteAccess Opened             | 18043              | Indicates that a remote access connection was established. | 1                              |
| RemoteAccess Closed             | 18044              | Indicates that a remote access connection was closed.      | 1                              |
| RemoteAccess Reset              | 18045              | Indicates that a remote access connection was reset.       | 3                              |
| RemoteAccess Terminated         | 18046              | Indicates that a remote access connection was terminated.  | 4                              |
| RemoteAccess Denied             | 18047              | Indicates that a remote access connection was denied.      | 4                              |
| RemoteAccess In Progress        | 18048              | Indicates that a remote access connection is in progress.  | 1                              |
| RemoteAccess Delayed            | 18049              | Indicates that a remote access connection was delayed.     | 3                              |
| RemoteAccess Redirected         | 18050              | Indicates that a remote access connection was redirected.  | 3                              |
| VPN Opened                      | 18051              | Indicates that a VPN connection was opened.                | 1                              |
| VPN Closed                      | 18052              | Indicates that a VPN connection was closed.                | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                         | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------|--------------------------------|
| VPN Reset                       | 18053              | Indicates that a VPN connection was reset.                 | 3                              |
| VPN Terminated                  | 18054              | Indicates that a VPN connection was terminated.            | 4                              |
| VPN Denied                      | 18055              | Indicates that a VPN connection was denied.                | 4                              |
| VPN In Progress                 | 18056              | Indicates that a VPN connection is in progress.            | 1                              |
| VPN Delayed                     | 18057              | Indicates that a VPN connection was delayed                | 3                              |
| VPN Queued                      | 18058              | Indicates that a VPN connection was queued.                | 3                              |
| VPN Redirected                  | 18059              | Indicates that a VPN connection was redirected.            | 3                              |
| RDP Opened                      | 18060              | Indicates that an RDP connection was established.          | 1                              |
| RDP Closed                      | 18061              | Indicates that an RDP connection was closed.               | 1                              |
| RDP Reset                       | 18062              | Indicates that an RDP connection was reset.                | 3                              |
| RDP Terminated                  | 18063              | Indicates that an RDP connection was terminated.           | 4                              |
| RDP Denied                      | 18064              | Indicates that an RDP connection was denied.               | 4                              |
| RDP In Progress                 | 18065              | Indicates that an RDP connection is in progress.           | 1                              |
| RDP Redirected                  | 18066              | Indicates that an RDP connection was redirected.           | 3                              |
| FileTransfer Opened             | 18067              | Indicates that a file transfer connection was established. | 1                              |
| FileTransfer Closed             | 18068              | Indicates that a file transfer connection was closed.      | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                        | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------|--------------------------------|
| FileTransfer Reset              | 18069              | Indicates that a file transfer connection was reset.      | 3                              |
| FileTransfer Terminated         | 18070              | Indicates that a file transfer connection was terminated. | 4                              |
| FileTransfer Denied             | 18071              | Indicates that a file transfer connection was denied.     | 4                              |
| FileTransfer In Progress        | 18072              | Indicates that a file transfer connection is in progress. | 1                              |
| FileTransfer Delayed            | 18073              | Indicates that a file transfer connection was delayed.    | 3                              |
| FileTransfer Queued             | 18074              | Indicates that a file transfer connection was queued.     | 3                              |
| FileTransfer Redirected         | 18075              | Indicates that a file transfer connection was redirected. | 3                              |
| DNS Opened                      | 18076              | Indicates that a DNS connection was established.          | 1                              |
| DNS Closed                      | 18077              | Indicates that a DNS connection was closed.               | 1                              |
| DNS Reset                       | 18078              | Indicates that a DNS connection was reset.                | 5                              |
| DNS Terminated                  | 18079              | Indicates that a DNS connection was terminated.           | 5                              |
| DNS Denied                      | 18080              | Indicates that a DNS connection was denied.               | 5                              |
| DNS In Progress                 | 18081              | Indicates that a DNS connection is in progress.           | 1                              |
| DNS Delayed                     | 18082              | Indicates that a DNS connection was delayed.              | 5                              |
| DNS Redirected                  | 18083              | Indicates that a DNS connection was redirected.           | 4                              |
| Chat Opened                     | 18084              | Indicates that a chat connection was opened.              | 1                              |



*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                    | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------|--------------------------------|
| Chat Closed                     | 18085              | Indicates that a chat connection was closed.          | 1                              |
| Chat Reset                      | 18086              | Indicates that a chat connection was reset.           | 3                              |
| Chat Terminated                 | 18087              | Indicates that a chat connection was terminated.      | 3                              |
| Chat Denied                     | 18088              | Indicates that a chat connection was denied.          | 3                              |
| Chat In Progress                | 18089              | Indicates that a chat connection is in progress.      | 1                              |
| Chat Redirected                 | 18090              | Indicates that a chat connection was redirected.      | 1                              |
| Database Opened                 | 18091              | Indicates that a database connection was established. | 1                              |
| Database Closed                 | 18092              | Indicates that a database connection was closed.      | 1                              |
| Database Reset                  | 18093              | Indicates that a database connection was reset.       | 5                              |
| Database Terminated             | 18094              | Indicates that a database connection was terminated.  | 5                              |
| Database Denied                 | 18095              | Indicates that a database connection was denied.      | 5                              |
| Database In Progress            | 18096              | Indicates that a database connection is in progress.  | 1                              |
| Database Redirected             | 18097              | Indicates that a database connection was redirected.  | 3                              |
| SMTP Opened                     | 18098              | Indicates that an SMTP connection was established.    | 1                              |
| SMTP Closed                     | 18099              | Indicates that an SMTP connection was closed.         | 1                              |
| SMTP Reset                      | 18100              | Indicates that an SMTP connection was reset.          | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                 | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------------------|--------------------------------|
| SMTP Terminated                 | 18101              | Indicates that an SMTP connection was terminated.                  | 5                              |
| SMTP Denied                     | 18102              | Indicates that an SMTP connection was denied.                      | 5                              |
| SMTP In Progress                | 18103              | Indicates that an SMTP connection is in progress.                  | 1                              |
| SMTP Delayed                    | 18104              | Indicates that an SMTP connection was delayed.                     | 3                              |
| SMTP Queued                     | 18105              | Indicates that an SMTP connection was queued.                      | 3                              |
| SMTP Redirected                 | 18106              | Indicates that an SMTP connection was redirected.                  | 3                              |
| Auth Opened                     | 18107              | Indicates that an authorization server connection was established. | 1                              |
| Auth Closed                     | 18108              | Indicates that an authorization server connection was closed.      | 1                              |
| Auth Reset                      | 18109              | Indicates that an authorization server connection was reset.       | 3                              |
| Auth Terminated                 | 18110              | Indicates that an authorization server connection was terminated.  | 4                              |
| Auth Denied                     | 18111              | Indicates that an authorization server connection was denied.      | 4                              |
| Auth In Progress                | 18112              | Indicates that an authorization server connection is in progress.  | 1                              |
| Auth Delayed                    | 18113              | Indicates that an authorization server connection was delayed.     | 3                              |
| Auth Queued                     | 18114              | Indicates that an authorization server connection was queued.      | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------------------|--------------------------------|
| Auth Redirected                 | 18115              | Indicates that an authorization server connection was redirected. | 2                              |
| P2P Opened                      | 18116              | Indicates that a Peer-to-Peer (P2P) connection was established.   | 1                              |
| P2P Closed                      | 18117              | Indicates that a P2P connection was closed.                       | 1                              |
| P2P Reset                       | 18118              | Indicates that a P2P connection was reset.                        | 4                              |
| P2P Terminated                  | 18119              | Indicates that a P2P connection was terminated.                   | 4                              |
| P2P Denied                      | 18120              | Indicates that a P2P connection was denied.                       | 3                              |
| P2P In Progress                 | 18121              | Indicates that a P2P connection is in progress.                   | 1                              |
| Web Opened                      | 18122              | Indicates that a web connection was established.                  | 1                              |
| Web Closed                      | 18123              | Indicates that a web connection was closed.                       | 1                              |
| Web Reset                       | 18124              | Indicates that a web connection was reset.                        | 4                              |
| Web Terminated                  | 18125              | Indicates that a web connection was terminated.                   | 4                              |
| Web Denied                      | 18126              | Indicates that a web connection was denied.                       | 4                              |
| Web In Progress                 | 18127              | Indicates that a web connection is in progress.                   | 1                              |
| Web Delayed                     | 18128              | Indicates that a web connection was delayed.                      | 3                              |
| Web Queued                      | 18129              | Indicates that a web connection was queued.                       | 1                              |
| Web Redirected                  | 18130              | Indicates that a web connection was redirected.                   | 1                              |
| Web Proxy                       | 18131              | Indicates that a web connection was proxied.                      | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                     | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|----------------------------------------------------------------------------------------|--------------------------------|
| VoIP Opened                     | 18132              | Indicates that a Voice Over IP (VoIP) connection was established.                      | 1                              |
| VoIP Closed                     | 18133              | Indicates that a VoIP connection was closed.                                           | 1                              |
| VoIP Reset                      | 18134              | Indicates that a VoIP connection was reset.                                            | 3                              |
| VoIP Terminated                 | 18135              | Indicates that a VoIP connection was terminated.                                       | 3                              |
| VoIP Denied                     | 18136              | Indicates that a VoIP connection was denied.                                           | 3                              |
| VoIP In Progress                | 18137              | Indicates that a VoIP connection is in progress.                                       | 1                              |
| VoIP Delayed                    | 18138              | Indicates that a VoIP connection was delayed.                                          | 3                              |
| VoIP Redirected                 | 18139              | Indicates that a VoIP connection was redirected.                                       | 3                              |
| LDAP Session Started            | 18140              | Indicates an LDAP session started.                                                     | 1                              |
| LDAP Session Ended              | 18141              | Indicates an LDAP session ended.                                                       | 1                              |
| LDAP Session Denied             | 18142              | Indicates that an LDAP session was denied.                                             | 3                              |
| LDAP Session Status             | 18143              | Indicates that an LDAP session status message was reported.                            | 1                              |
| LDAP Authentication Failed      | 18144              | Indicates that an LDAP authentication failed.                                          | 4                              |
| LDAP Authentication Succeeded   | 18145              | Indicates that an LDAP authentication was successful.                                  | 1                              |
| AAA Session Started             | 18146              | Indicates that an Authentication, Authorization, and Accounting (AAA) session started. | 1                              |
| AAA Session Ended               | 18147              | Indicates that an AAA session ended.                                                   | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                          | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------------------|--------------------------------|
| AAA Session Denied              | 18148              | Indicates that an AAA session was denied.                                   | 3                              |
| AAA Session Status              | 18149              | Indicates that an AAA session status message was reported.                  | 1                              |
| AAA Authentication Failed       | 18150              | Indicates that an AAA authentication failed.                                | 4                              |
| AAA Authentication Succeeded    | 18151              | Indicates that an AAA authentication was successful.                        | 1                              |
| IPSEC Authentication Failed     | 18152              | Indicates that an Internet Protocol Security (IPSEC) authentication failed. | 4                              |
| IPSEC Authentication Succeeded  | 18153              | Indicates that an IPSEC authentication was successful.                      | 1                              |
| IPSEC Session Started           | 18154              | Indicates that an IPSEC session started.                                    | 1                              |
| IPSEC Session Ended             | 18155              | Indicates that an IPSEC session ended.                                      | 1                              |
| IPSEC Error                     | 18156              | Indicates that an IPSEC error message was reported.                         | 5                              |
| IPSEC Status                    | 18157              | Indicates that an IPSEC session status message was reported.                | 1                              |
| IM Session Opened               | 18158              | Indicates that an Instant Messenger (IM) session was established.           | 1                              |
| IM Session Closed               | 18159              | Indicates that an IM session was closed.                                    | 1                              |
| IM Session Reset                | 18160              | Indicates that an IM session was reset.                                     | 3                              |
| IM Session Terminated           | 18161              | Indicates that an IM session was terminated.                                | 3                              |
| IM Session Denied               | 18162              | Indicates that an IM session was denied.                                    | 3                              |
| IM Session In Progress          | 18163              | Indicates that an IM session is in progress.                                | 1                              |
| IM Session Delayed              | 18164              | Indicates that an IM session was delayed                                    | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                                                                                       | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| IM Session Redirected           | 18165              | Indicates that an IM session was redirected.                                                                                                             | 3                              |
| WHOIS Session Opened            | 18166              | Indicates that a WHOIS session was established.                                                                                                          | 1                              |
| WHOIS Session Closed            | 18167              | Indicates that a WHOIS session was closed.                                                                                                               | 1                              |
| WHOIS Session Reset             | 18168              | Indicates that a WHOIS session was reset.                                                                                                                | 3                              |
| WHOIS Session Terminated        | 18169              | Indicates that a WHOIS session was terminated.                                                                                                           | 3                              |
| WHOIS Session Denied            | 18170              | Indicates that a WHOIS session was denied.                                                                                                               | 3                              |
| WHOIS Session In Progress       | 18171              | Indicates that a WHOIS session is in progress.                                                                                                           | 1                              |
| WHOIS Session Redirected        | 18172              | Indicates that a WHOIS session was redirected.                                                                                                           | 3                              |
| Traceroute Session Opened       | 18173              | Indicates that a Traceroute session was established.                                                                                                     | 1                              |
| Traceroute Session Closed       | 18174              | Indicates that a Traceroute session was closed.                                                                                                          | 1                              |
| Traceroute Session Denied       | 18175              | Indicates that a Traceroute session was denied.                                                                                                          | 3                              |
| Traceroute Session In Progress  | 18176              | Indicates that a Traceroute session is in progress.                                                                                                      | 1                              |
| TN3270 Session Opened           | 18177              | TN3270 is a terminal emulation program, which is used to connect to an IBM 3270 terminal. This category indicates that a TN3270 session was established. | 1                              |
| TN3270 Session Closed           | 18178              | Indicates that a TN3270 session was closed.                                                                                                              | 1                              |
| TN3270 Session Reset            | 18179              | Indicates that a TN3270 session was reset.                                                                                                               | 3                              |
| TN3270 Session Terminated       | 18180              | Indicates that a TN3270 session was terminated.                                                                                                          | 3                              |
| TN3270 Session Denied           | 18181              | Indicates that a TN3270 session was denied.                                                                                                              | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                  | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|---------------------------------------------------------------------|--------------------------------|
| TN3270 Session In Progress      | 18182              | Indicates that a TN3270 session is in progress.                     | 1                              |
| TFTP Session Opened             | 18183              | Indicates that a TFTP session was established.                      | 1                              |
| TFTP Session Closed             | 18184              | Indicates that a TFTP session was closed.                           | 1                              |
| TFTP Session Reset              | 18185              | Indicates that a TFTP session was reset.                            | 3                              |
| TFTP Session Terminated         | 18186              | Indicates that a TFTP session was terminated.                       | 3                              |
| TFTP Session Denied             | 18187              | Indicates that a TFTP session was denied.                           | 3                              |
| TFTP Session In Progress        | 18188              | Indicates that a TFTP session is in progress.                       | 1                              |
| Telnet Session Opened           | 18189              | Indicates that a Telnet session was established.                    | 1                              |
| Telnet Session Closed           | 18190              | Indicates that a Telnet session was closed.                         | 1                              |
| Telnet Session Reset            | 18191              | Indicates that a Telnet session was reset.                          | 3                              |
| Telnet Session Terminated       | 18192              | Indicates that a Telnet session was terminated.                     | 3                              |
| Telnet Session Denied           | 18193              | Indicates that a Telnet session was denied.                         | 3                              |
| Telnet Session In Progress      | 18194              | Indicates that a Telnet session is in progress.                     | 1                              |
| Syslog Session Opened           | 18201              | Indicates that a syslog session was established.                    | 1                              |
| Syslog Session Closed           | 18202              | Indicates that a syslog session was closed.                         | 1                              |
| Syslog Session Denied           | 18203              | Indicates that a syslog session was denied.                         | 3                              |
| Syslog Session In Progress      | 18204              | Indicates that a syslog session is in progress.                     | 1                              |
| SSL Session Opened              | 18205              | Indicates that a Secure Socket Layer (SSL) session was established. | 1                              |
| SSL Session Closed              | 18206              | Indicates that an SSL session was closed.                           | 1                              |
| SSL Session Reset               | 18207              | Indicates that an SSL session was reset.                            | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b>    | <b>Category ID</b> | <b>Description</b>                                                                  | <b>Severity level (0 - 10)</b> |
|------------------------------------|--------------------|-------------------------------------------------------------------------------------|--------------------------------|
| SSL Session Terminated             | 18208              | Indicates that an SSL session was terminated.                                       | 3                              |
| SSL Session Denied                 | 18209              | Indicates that an SSL session was denied.                                           | 3                              |
| SSL Session In Progress            | 18210              | Indicates that an SSL session is in progress.                                       | 1                              |
| SNMP Session Opened                | 18211              | Indicates that a Simple Network Management Protocol (SNMP) session was established. | 1                              |
| SNMP Session Closed                | 18212              | Indicates that an SNMP session was closed.                                          | 1                              |
| SNMP Session Denied                | 18213              | Indicates that an SNMP session was denied.                                          | 3                              |
| SNMP Session In Progress           | 18214              | Indicates that an SNMP session is in progress.                                      | 1                              |
| SMB Session Opened                 | 18215              | Indicates that a Server Message Block (SMB) session was established.                | 1                              |
| SMB Session Closed                 | 18216              | Indicates that an SMB session was closed.                                           | 1                              |
| SMB Session Reset                  | 18217              | Indicates that an SMB session was reset.                                            | 3                              |
| SMB Session Terminated             | 18218              | Indicates that an SMB session was terminated.                                       | 3                              |
| SMB Session Denied                 | 18219              | Indicates that an SMB session was denied.                                           | 3                              |
| SMB Session In Progress            | 18220              | Indicates that an SMB session is in progress.                                       | 1                              |
| Streaming Media Session Opened     | 18221              | Indicates that a Streaming Media session was established.                           | 1                              |
| Streaming Media Session Closed     | 18222              | Indicates that a Streaming Media session was closed.                                | 1                              |
| Streaming Media Session Reset      | 18223              | Indicates that a Streaming Media session was reset.                                 | 3                              |
| Streaming Media Session Terminated | 18224              | Indicates that a Streaming Media session was terminated.                            | 3                              |



*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b>     | <b>Category ID</b> | <b>Description</b>                                              | <b>Severity level (0 - 10)</b> |
|-------------------------------------|--------------------|-----------------------------------------------------------------|--------------------------------|
| Streaming Media Session Denied      | 18225              | Indicates that a Streaming Media session was denied.            | 3                              |
| Streaming Media Session In Progress | 18226              | Indicates that a Streaming Media session is in progress.        | 1                              |
| RUSERS Session Opened               | 18227              | Indicates that a (Remote Users) RUSERS session was established. | 1                              |
| RUSERS Session Closed               | 18228              | Indicates that a RUSERS session was closed.                     | 1                              |
| RUSERS Session Denied               | 18229              | Indicates that a RUSERS session was denied.                     | 3                              |
| RUSERS Session In Progress          | 18230              | Indicates that a RUSERS session is in progress.                 | 1                              |
| Rsh Session Opened                  | 18231              | Indicates that a remote shell (rsh) session was established.    | 1                              |
| Rsh Session Closed                  | 18232              | Indicates that an rsh session was closed.                       | 1                              |
| Rsh Session Reset                   | 18233              | Indicates that an rsh session was reset.                        | 3                              |
| Rsh Session Terminated              | 18234              | Indicates that an rsh session was terminated.                   | 3                              |
| Rsh Session Denied                  | 18235              | Indicates that an rsh session was denied.                       | 3                              |
| Rsh Session In Progress             | 18236              | Indicates that an rsh session is in progress.                   | 1                              |
| RLOGIN Session Opened               | 18237              | Indicates that a Remote Login (RLOGIN) session was established. | 1                              |
| RLOGIN Session Closed               | 18238              | Indicates that an RLOGIN session was closed.                    | 1                              |
| RLOGIN Session Reset                | 18239              | Indicates that an RLOGIN session was reset.                     | 3                              |
| RLOGIN Session Terminated           | 18240              | Indicates that an RLOGIN session was terminated.                | 3                              |
| RLOGIN Session Denied               | 18241              | Indicates that an RLOGIN session was denied.                    | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                    | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------------|--------------------------------|
| RLOGIN Session In Progress      | 18242              | Indicates that an RLOGIN session is in progress.                      | 1                              |
| REXEC Session Opened            | 18243              | Indicates that a (Remote Execution) REXEC session was established.    | 1                              |
| REXEC Session Closed            | 18244              | Indicates that an REXEC session was closed.                           | 1                              |
| REXEC Session Reset             | 18245              | Indicates that an REXEC session was reset.                            | 3                              |
| REXEC Session Terminated        | 18246              | Indicates that an REXEC session was terminated.                       | 3                              |
| REXEC Session Denied            | 18247              | Indicates that an REXEC session was denied.                           | 3                              |
| REXEC Session In Progress       | 18248              | Indicates that an REXEC session is in progress.                       | 1                              |
| RPC Session Opened              | 18249              | Indicates that a Remote Procedure Call (RPC) session was established. | 1                              |
| RPC Session Closed              | 18250              | Indicates that an RPC session was closed.                             | 1                              |
| RPC Session Reset               | 18251              | Indicates that an RPC session was reset.                              | 3                              |
| RPC Session Terminated          | 18252              | Indicates that an RPC session was terminated.                         | 3                              |
| RPC Session Denied              | 18253              | Indicates that an RPC session was denied.                             | 3                              |
| RPC Session In Progress         | 18254              | Indicates that an RPC session is in progress.                         | 1                              |
| NTP Session Opened              | 18255              | Indicates that a Network Time Protocol (NTP) session was established. | 1                              |
| NTP Session Closed              | 18256              | Indicates that an NTP session was closed.                             | 1                              |
| NTP Session Reset               | 18257              | Indicates that an NTP session was reset.                              | 3                              |
| NTP Session Terminated          | 18258              | Indicates that an NTP session was terminated.                         | 3                              |
| NTP Session Denied              | 18259              | Indicates that an NTP session was denied.                             | 3                              |
| NTP Session In Progress         | 18260              | Indicates that an NTP session is in progress.                         | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                              | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|---------------------------------------------------------------------------------|--------------------------------|
| NNTP Session Opened             | 18261              | Indicates that a Network News Transfer Protocol (NNTP) session was established. | 1                              |
| NNTP Session Closed             | 18262              | Indicates that an NNTP session was closed.                                      | 1                              |
| NNTP Session Reset              | 18263              | Indicates that an NNTP session was reset.                                       | 3                              |
| NNTP Session Terminated         | 18264              | Indicates that an NNTP session was terminated.                                  | 3                              |
| NNTP Session Denied             | 18265              | Indicates that an NNTP session was denied.                                      | 3                              |
| NNTP Session In Progress        | 18266              | Indicates that an NNTP session is in progress.                                  | 1                              |
| NFS Session Opened              | 18267              | Indicates that a Network File System (NFS) session was established.             | 1                              |
| NFS Session Closed              | 18268              | Indicates that an NFS session was closed.                                       | 1                              |
| NFS Session Reset               | 18269              | Indicates that an NFS session was reset.                                        | 3                              |
| NFS Session Terminated          | 18270              | Indicates that an NFS session was terminated.                                   | 3                              |
| NFS Session Denied              | 18271              | Indicates that an NFS session was denied.                                       | 3                              |
| NFS Session In Progress         | 18272              | Indicates that an NFS session is in progress.                                   | 1                              |
| NCP Session Opened              | 18273              | Indicates that a Network Control Program (NCP) session was established.         | 1                              |
| NCP Session Closed              | 18274              | Indicates that an NCP session was closed.                                       | 1                              |
| NCP Session Reset               | 18275              | Indicates that an NCP session was reset.                                        | 3                              |
| NCP Session Terminated          | 18276              | Indicates that an NCP session was terminated.                                   | 3                              |
| NCP Session Denied              | 18277              | Indicates that an NCP session was denied.                                       | 3                              |
| NCP Session In Progress         | 18278              | Indicates that an NCP session is in progress.                                   | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                  | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|---------------------------------------------------------------------|--------------------------------|
| NetBIOS Session Opened          | 18279              | Indicates that a NetBIOS session was established.                   | 1                              |
| NetBIOS Session Closed          | 18280              | Indicates that a NetBIOS session was closed.                        | 1                              |
| NetBIOS Session Reset           | 18281              | Indicates that a NetBIOS session was reset.                         | 3                              |
| NetBIOS Session Terminated      | 18282              | Indicates that a NetBIOS session was terminated.                    | 3                              |
| NetBIOS Session Denied          | 18283              | Indicates that a NetBIOS session was denied.                        | 3                              |
| NetBIOS Session In Progress     | 18284              | Indicates that a NetBIOS session is in progress.                    | 1                              |
| MODBUS Session Opened           | 18285              | Indicates that a MODBUS session was established.                    | 1                              |
| MODBUS Session Closed           | 18286              | Indicates that a MODBUS session was closed.                         | 1                              |
| MODBUS Session Reset            | 18287              | Indicates that a MODBUS session was reset.                          | 3                              |
| MODBUS Session Terminated       | 18288              | Indicates that a MODBUS session was terminated.                     | 3                              |
| MODBUS Session Denied           | 18289              | Indicates that a MODBUS session was denied.                         | 3                              |
| MODBUS Session In Progress      | 18290              | Indicates that a MODBUS session is in progress.                     | 1                              |
| LPD Session Opened              | 18291              | Indicates that a Line Printer Daemon (LPD) session was established. | 1                              |
| LPD Session Closed              | 18292              | Indicates that an LPD session was closed.                           | 1                              |
| LPD Session Reset               | 18293              | Indicates that an LPD session was reset.                            | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                    | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------|--------------------------------|
| LPD Session Terminated          | 18294              | Indicates that an LPD session was terminated.         | 3                              |
| LPD Session Denied              | 18295              | Indicates that an LPD session was denied.             | 3                              |
| LPD Session In Progress         | 18296              | Indicates that an LPD session is in progress.         | 1                              |
| Lotus Notes® Session Opened     | 18297              | Indicates that a Lotus Notes session was established. | 1                              |
| Lotus Notes Session Closed      | 18298              | Indicates that a Lotus Notes session was closed.      | 1                              |
| Lotus Notes Session Reset       | 18299              | Indicates that a Lotus Notes session was reset.       | 3                              |
| Lotus Notes Session Terminated  | 18300              | Indicates that a Lotus Notes session was terminated.  | 3                              |
| Lotus Notes Session Denied      | 18301              | Indicates that a Lotus Notes session was denied.      | 3                              |
| Lotus Notes Session In Progress | 18302              | Indicates that a Lotus Notes session is in progress.  | 1                              |
| Kerberos Session Opened         | 18303              | Indicates that a Kerberos session was established.    | 1                              |
| Kerberos Session Closed         | 18304              | Indicates that a Kerberos session was closed.         | 1                              |
| Kerberos Session Reset          | 18305              | Indicates that a Kerberos session was reset.          | 3                              |
| Kerberos Session Terminated     | 18306              | Indicates that a Kerberos session was terminated.     | 3                              |
| Kerberos Session Denied         | 18307              | Indicates that a Kerberos session was denied.         | 3                              |
| Kerberos Session In Progress    | 18308              | Indicates that a Kerberos session is in progress.     | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                             | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------------------------------|--------------------------------|
| IRC Session Opened              | 18309              | Indicates that an Internet Relay Chat (IRC) session was established.           | 1                              |
| IRC Session Closed              | 18310              | Indicates that an IRC session was closed.                                      | 1                              |
| IRC Session Reset               | 18311              | Indicates that an IRC session was reset.                                       | 3                              |
| IRC Session Terminated          | 18312              | Indicates that an IRC session was terminated.                                  | 3                              |
| IRC Session Denied              | 18313              | Indicates that an IRC session was denied.                                      | 3                              |
| IRC Session In Progress         | 18314              | Indicates that an IRC session is in progress.                                  | 1                              |
| IEC 104 Session Opened          | 18315              | Indicates that an IEC 104 session was established.                             | 1                              |
| IEC 104 Session Closed          | 18316              | Indicates that an IEC 104 session was closed.                                  | 1                              |
| IEC 104 Session Reset           | 18317              | Indicates that an IEC 104 session was reset.                                   | 3                              |
| IEC 104 Session Terminated      | 18318              | Indicates that an IEC 104 session was terminated.                              | 3                              |
| IEC 104 Session Denied          | 18319              | Indicates that an IEC 104 session was denied.                                  | 3                              |
| IEC 104 Session In Progress     | 18320              | Indicates that an IEC 104 session is in progress.                              | 1                              |
| Ident Session Opened            | 18321              | Indicates that a TCP Client Identity Protocol (Ident) session was established. | 1                              |
| Ident Session Closed            | 18322              | Indicates that an Ident session was closed.                                    | 1                              |
| Ident Session Reset             | 18323              | Indicates that an Ident session was reset.                                     | 3                              |
| Ident Session Terminated        | 18324              | Indicates that an Ident session was terminated.                                | 3                              |
| Ident Session Denied            | 18325              | Indicates that an Ident session was denied.                                    | 3                              |
| Ident Session In Progress       | 18326              | Indicates that an Ident session is in progress.                                | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                             | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------------------------------------------|--------------------------------|
| ICCP Session Opened             | 18327              | Indicates that an Inter-Control Center Communications Protocol (ICCP) session was established. | 1                              |
| ICCP Session Closed             | 18328              | Indicates that an ICCP session was closed.                                                     | 1                              |
| ICCP Session Reset              | 18329              | Indicates that an ICCP session was reset.                                                      | 3                              |
| ICCP Session Terminated         | 18330              | Indicates that an ICCP session was terminated.                                                 | 3                              |
| ICCP Session Denied             | 18331              | Indicates that an ICCP session was denied.                                                     | 3                              |
| ICCP Session In Progress        | 18332              | Indicates that an ICCP session is in progress.                                                 | 1                              |
| GroupWiseSession Opened         | 18333              | Indicates that a GroupWisesession was established.                                             | 1                              |
| GroupWiseSession Closed         | 18334              | Indicates that a GroupWise session was closed.                                                 | 1                              |
| GroupWiseSession Reset          | 18335              | Indicates that a GroupWisesession was reset.                                                   | 3                              |
| GroupWiseSession Terminated     | 18336              | Indicates that a GroupWisesession was terminated.                                              | 3                              |
| GroupWiseSession Denied         | 18337              | Indicates that a GroupWise session was denied.                                                 | 3                              |
| GroupWiseSession In Progress    | 18338              | Indicates that a GroupWise session is in progress.                                             | 1                              |
| Gopher Session Opened           | 183398             | Indicates that a Gopher session was established.                                               | 1                              |
| Gopher Session Closed           | 18340              | Indicates that a Gopher session was closed.                                                    | 1                              |
| Gopher Session Reset            | 18341              | Indicates that a Gopher session was reset.                                                     | 3                              |
| Gopher Session Terminated       | 18342              | Indicates that a Gopher session was terminated.                                                | 3                              |
| Gopher Session Denied           | 18343              | Indicates that a Gopher session was denied.                                                    | 3                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                          | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-----------------------------------------------------------------------------|--------------------------------|
| Gopher Session In Progress      | 18344              | Indicates that a Gopher session is in progress.                             | 1                              |
| GIOP Session Opened             | 18345              | Indicates that a General Inter-ORB Protocol (GIOP) session was established. | 1                              |
| GIOP Session Closed             | 18346              | Indicates that a GIOP session was closed.                                   | 1                              |
| GIOP Session Reset              | 18347              | Indicates that a GIOP session was reset.                                    | 3                              |
| GIOP Session Terminated         | 18348              | Indicates that a GIOP session was terminated.                               | 3                              |
| GIOP Session Denied             | 18349              | Indicates that a GIOP session was denied.                                   | 3                              |
| GIOP Session In Progress        | 18350              | Indicates that a GIOP session is in progress.                               | 1                              |
| Finger Session Opened           | 18351              | Indicates that a Finger session was established.                            | 1                              |
| Finger Session Closed           | 18352              | Indicates that a Finger session was closed.                                 | 1                              |
| Finger Session Reset            | 18353              | Indicates that a Finger session was reset.                                  | 3                              |
| Finger Session Terminated       | 18354              | Indicates that a Finger session was terminated.                             | 3                              |
| Finger Session Denied           | 18355              | Indicates that a Finger session was denied.                                 | 3                              |
| Finger Session In Progress      | 18356              | Indicates that a Finger session is in progress.                             | 1                              |
| Echo Session Opened             | 18357              | Indicates that an Echo session was established.                             | 1                              |
| Echo Session Closed             | 18358              | Indicates that an Echo session was closed.                                  | 1                              |
| Echo Session Denied             | 18359              | Indicates that an Echo session was denied.                                  | 3                              |
| Echo Session In Progress        | 18360              | Indicates that an Echo session is in progress.                              | 1                              |
| Remote .NET Session Opened      | 18361              | Indicates that a Remote .NET session was established.                       | 1                              |
| Remote .NET Session Closed      | 18362              | Indicates that a Remote .NET session was closed.                            | 1                              |



*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                                   | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|--------------------------------------------------------------------------------------|--------------------------------|
| Remote .NET Session Reset       | 18363              | Indicates that a Remote .NET session was reset.                                      | 3                              |
| Remote .NET Session Terminated  | 18364              | Indicates that a Remote .NET session was terminated.                                 | 3                              |
| Remote .NET Session Denied      | 18365              | Indicates that a Remote .NET session was denied.                                     | 3                              |
| Remote .NET Session In Progress | 18366              | Indicates that a Remote .NET session is in progress.                                 | 1                              |
| DNP3 Session Opened             | 18367              | Indicates that a Distributed Network Proctologic (DNP3) session was established.     | 1                              |
| DNP3 Session Closed             | 18368              | Indicates that a DNP3 session was closed.                                            | 1                              |
| DNP3 Session Reset              | 18369              | Indicates that a DNP3 session was reset.                                             | 3                              |
| DNP3 Session Terminated         | 18370              | Indicates that a DNP3 session was terminated.                                        | 3                              |
| DNP3 Session Denied             | 18371              | Indicates that a DNP3 session was denied.                                            | 3                              |
| DNP3 Session In Progress        | 18372              | Indicates that a DNP3 session is in progress.                                        | 1                              |
| Discard Session Opened          | 18373              | Indicates that a Discard session was established.                                    | 1                              |
| Discard Session Closed          | 18374              | Indicates that a Discard session was closed.                                         | 1                              |
| Discard Session Reset           | 18375              | Indicates that a Discard session was reset.                                          | 3                              |
| Discard Session Terminated      | 18376              | Indicates that a Discard session was terminated.                                     | 3                              |
| Discard Session Denied          | 18377              | Indicates that a Discard session was denied.                                         | 3                              |
| Discard Session In Progress     | 18378              | Indicates that a Discard session is in progress.                                     | 1                              |
| DHCP Session Opened             | 18379              | Indicates that a Dynamic Host Configuration Protocol (DHCP) session was established. | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                           | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|------------------------------------------------------------------------------|--------------------------------|
| DHCP Session Closed             | 18380              | Indicates that a DHCP session was closed.                                    | 1                              |
| DHCP Session Denied             | 18381              | Indicates that a DHCP session was denied.                                    | 3                              |
| DHCP Session In Progress        | 18382              | Indicates that a DHCP session is in progress.                                | 1                              |
| DHCP Success                    | 18383              | Indicates that a DHCP lease was successfully obtained                        | 1                              |
| DHCP Failure                    | 18384              | Indicates that a DHCP lease cannot be obtained.                              | 3                              |
| CVS Session Opened              | 18385              | Indicates that a Concurrent Versions System (CVS) session was established.   | 1                              |
| CVS Session Closed              | 18386              | Indicates that a CVS session was closed.                                     | 1                              |
| CVS Session Reset               | 18387              | Indicates that a CVS session was reset.                                      | 3                              |
| CVS Session Terminated          | 18388              | Indicates that a CVS session was terminated.                                 | 3                              |
| CVS Session Denied              | 18389              | Indicates that a CVS session was denied.                                     | 3                              |
| CVS Session In Progress         | 18390              | Indicates that a CVS session is in progress.                                 | 1                              |
| CUPS Session Opened             | 18391              | Indicates that a Common UNIX Printing System (CUPS) session was established. | 1                              |
| CUPS Session Closed             | 18392              | Indicates that a CUPS session was closed.                                    | 1                              |
| CUPS Session Reset              | 18393              | Indicates that a CUPS session was reset.                                     | 3                              |
| CUPS Session Terminated         | 18394              | Indicates that a CUPS session was terminated.                                | 3                              |
| CUPS Session Denied             | 18395              | Indicates that a CUPS session was denied.                                    | 3                              |
| CUPS Session In Progress        | 18396              | Indicates that a CUPS session is in progress.                                | 1                              |

*Table 55. Low-level categories and severity levels for the application category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                                  | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|---------------------------------------------------------------------|--------------------------------|
| Chargen Session Started         | 18397              | Indicates that a Character Generator (Chargen) session was started. | 1                              |
| Chargen Session Closed          | 18398              | Indicates that a Chargen session was closed.                        | 1                              |
| Chargen Session Reset           | 18399              | Indicates that a Chargen session was reset.                         | 3                              |
| Chargen Session Terminated      | 18400              | Indicates that a Chargen session was terminated.                    | 3                              |
| Chargen Session Denied          | 18401              | Indicates that a Chargen session was denied.                        | 3                              |
| Chargen Session In Progress     | 18402              | Indicates that a Chargen session is in progress.                    | 1                              |
| Misc VPN                        | 18403              | Indicates that a miscellaneous VPN session was detected             | 1                              |
| DAP Session Started             | 18404              | Indicates that a DAP session was established.                       | 1                              |
| DAP Session Ended               | 18405              | Indicates that a DAP session ended.                                 | 1                              |
| DAP Session Denied              | 18406              | Indicates that a DAP session was denied.                            | 3                              |
| DAP Session Status              | 18407              | Indicates that a DAP session status request was made.               | 1                              |
| DAP Session in Progress         | 18408              | Indicates that a DAP session is in progress.                        | 1                              |
| DAP Authentication Failed       | 18409              | Indicates that a DAP authentication failed.                         | 4                              |
| DAP Authentication Succeeded    | 18410              | Indicates that DAP authentication succeeded.                        | 1                              |
| TOR Session Started             | 18411              | Indicates that a TOR session was established.                       | 1                              |
| TOR Session Closed              | 18412              | Indicates that a TOR session was closed.                            | 1                              |
| TOR Session Reset               | 18413              | Indicates that a TOR session was reset.                             | 3                              |
| TOR Session Terminated          | 18414              | Indicates that a TOR session was terminated.                        | 3                              |

Table 55. Low-level categories and severity levels for the application category (continued)

| Low-level event category | Category ID | Description                                                                    | Severity level (0 - 10) |
|--------------------------|-------------|--------------------------------------------------------------------------------|-------------------------|
| TOR Session Denied       | 18415       | Indicates that a TOR session was denied.                                       | 3                       |
| TOR Session In Progress  | 18416       | Indicates that a TOR session is in progress.                                   | 1                       |
| Game Session Started     | 18417       | Indicates that a game session was started.                                     | 1                       |
| Game Session Closed      | 18418       | Indicates that a game session was closed.                                      | 1                       |
| Game Session Reset       | 18419       | Indicates that a game session was reset.                                       | 3                       |
| Game Session Terminated  | 18420       | Indicates that a game session was terminated.                                  | 3                       |
| Game Session Denied      | 18421       | Indicates that a game session was denied.                                      | 3                       |
| Game Session In Progress | 18422       | Indicates that a game session is in progress.                                  | 1                       |
| Admin Login Attempt      | 18423       | Indicates that an attempt to log in as an administrative user was detected.    | 2                       |
| User Login Attempt       | 18424       | Indicates that an attempt to log in as a non-administrative user was detected. | 2                       |
| Client Server            | 18425       | Indicates client/server activity.                                              | 1                       |
| Content Delivery         | 18426       | Indicates content delivery activity.                                           | 1                       |
| Data Transfer            | 18427       | Indicates a data transfer.                                                     | 3                       |
| Data Warehousing         | 18428       | Indicates data warehousing activity.                                           | 3                       |
| Directory Services       | 18429       | Indicates directory service activity.                                          | 2                       |
| File Print               | 18430       | Indicates file print activity.                                                 | 1                       |
| File Transfer            | 18431       | Indicates file transfer.                                                       | 2                       |
| Games                    | 18432       | Indicates game activity.                                                       | 4                       |
| Healthcare               | 18433       | Indicates healthcare activity.                                                 | 1                       |
| Inner System             | 18434       | Indicates inner system activity.                                               | 1                       |

| <i>Table 55. Low-level categories and severity levels for the application category (continued)</i> |                    |                                        |                                |
|----------------------------------------------------------------------------------------------------|--------------------|----------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                    | <b>Category ID</b> | <b>Description</b>                     | <b>Severity level (0 - 10)</b> |
| Internet Protocol                                                                                  | 18435              | Indicates Internet Protocol activity.  | 1                              |
| Legacy                                                                                             | 18436              | Indicates legacy activity.             | 1                              |
| Mail                                                                                               | 18437              | Indicates mail activity.               | 1                              |
| Misc                                                                                               | 18438              | Indicates miscellaneous activity.      | 2                              |
| Multimedia                                                                                         | 18439              | Indicates multimedia activity.         | 2                              |
| Network Management                                                                                 | 18440              | Indicates network management activity. |                                |
| P2P                                                                                                | 18441              | Indicates Peer-to-Peer (P2P) activity. | 4                              |
| Remote Access                                                                                      | 18442              | Indicates Remote Access activity.      | 3                              |
| Routing Protocols                                                                                  | 18443              | Indicates routing protocol activity.   | 1                              |
| Security Protocols                                                                                 | 18444              | Indicates security protocol activity.  | 2                              |
| Streaming                                                                                          | 18445              | Indicates streaming activity.          | 2                              |
| Uncommon Protocol                                                                                  | 18446              | Indicates uncommon protocol activity.  | 3                              |
| VoIP                                                                                               | 18447              | Indicates VoIP activity.               | 1                              |
| Web                                                                                                | 18448              | Indicates web activity.                | 1                              |
| ICMP                                                                                               | 18449              | Indicates ICMP activity                | 1                              |

## Audit

The audit category contains events that are related to audit activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the audit category.

| <i>Table 56. Low-level categories and severity levels for the audit category</i> |                    |                                                   |                                |
|----------------------------------------------------------------------------------|--------------------|---------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                  | <b>Category ID</b> | <b>Description</b>                                | <b>Severity level (0 - 10)</b> |
| General Audit Event                                                              | 19001              | Indicates that a general audit event was started. | 1                              |
| Built-in Execution                                                               | 19002              | Indicates that a built-in audit task was run.     | 1                              |
| Bulk Copy                                                                        | 19003              | Indicates that a bulk copy of data was detected.  | 1                              |

Table 56. Low-level categories and severity levels for the audit category (continued)

| Low-level event category    | Category ID | Description                                                                 | Severity level (0 - 10) |
|-----------------------------|-------------|-----------------------------------------------------------------------------|-------------------------|
| Data Dump                   | 19004       | Indicates that a data dump was detected.                                    | 1                       |
| Data Import                 | 19005       | Indicates that a data import was detected.                                  | 1                       |
| Data Selection              | 19006       | Indicates that a data selection process was detected.                       | 1                       |
| Data Truncation             | 19007       | Indicates that the data truncation process was detected.                    | 1                       |
| Data Update                 | 19008       | Indicates that the data update process was detected.                        | 1                       |
| Procedure/Trigger Execution | 19009       | Indicates that the database procedure or trigger execution was detected.    | 1                       |
| Schema Change               | 19010       | Indicates that the schema for a procedure or trigger execution was altered. | 1                       |
| Create Activity Attempted   | 19011       | Indicates that creating activity was attempted.                             | 1                       |
| Create Activity Succeeded   | 19012       | Indicates that creating activity was successful.                            | 1                       |
| Create Activity Failed      | 19013       | Indicates that creating activity failed.                                    | 3                       |
| Read Activity Attempted     | 19014       | Indicates that a reading activity was attempted.                            | 1                       |
| Read Activity Succeeded     | 19015       | Indicates that a reading activity was successful.                           | 1                       |
| Read Activity Failed        | 19016       | Indicates that reading activity failed.                                     | 3                       |
| Update Activity Attempted   | 19017       | Indicates that updating activity was attempted.                             | 1                       |
| Update Activity Succeeded   | 19018       | Indicates that updating activity was successful.                            | 1                       |
| Update Activity Failed      | 19019       | Indicates that updating activity failed.                                    | 3                       |
| Delete Activity Attempted   | 19020       | Indicates that deleting activity was attempted.                             | 1                       |
| Delete Activity Succeeded   | 19021       | Indicates that deleting activity was successful.                            | 1                       |

*Table 56. Low-level categories and severity levels for the audit category (continued)*

| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                                    | <b>Severity level (0 - 10)</b> |
|---------------------------------|--------------------|-------------------------------------------------------|--------------------------------|
| Delete Activity Failed          | 19022              | Indicates that deleting activity failed.              | 3                              |
| Backup Activity Attempted       | 19023              | Indicates that backup activity was attempted.         | 1                              |
| Backup Activity Succeeded       | 19024              | Indicates that backup activity was successful.        | 1                              |
| Backup Activity Failed          | 19025              | Indicates that backup activity failed.                | 3                              |
| Capture Activity Attempted      | 19026              | Indicates that capturing activity was attempted.      | 1                              |
| Capture Activity Succeeded      | 19027              | Indicates that capturing activity was successful.     | 1                              |
| Capture Activity Failed         | 19028              | Indicates that capturing activity failed.             | 3                              |
| Configure Activity Attempted    | 19029              | Indicates that configuration activity was attempted.  | 1                              |
| Configure Activity Succeeded    | 19030              | Indicates that configuration activity was successful. | 1                              |
| Configure Activity Failed       | 19031              | Indicates that configuration activity failed.         | 3                              |
| Deploy Activity Attempted       | 19032              | Indicates that deployment activity was attempted.     | 1                              |
| Deploy Activity Succeeded       | 19033              | Indicates that deployment activity was successful.    | 1                              |
| Deploy Activity Failed          | 19034              | Indicates that deployment activity failed.            | 3                              |
| Disable Activity Attempted      | 19035              | Indicates that disabling activity was attempted.      | 1                              |
| Disable Activity Succeeded      | 19036              | Indicates that disabling activity was successful.     | 1                              |
| Disable Activity Failed         | 19037              | Indicates that disabling activity failed.             | 3                              |
| Enable Activity Attempted       | 19038              | Indicates that enabling activity was attempted.       | 1                              |
| Enable Activity Succeeded       | 19039              | Indicates that enabling activity was successful.      | 1                              |

Table 56. Low-level categories and severity levels for the audit category (continued)

| Low-level event category    | Category ID | Description                                        | Severity level (0 - 10) |
|-----------------------------|-------------|----------------------------------------------------|-------------------------|
| Enable Activity Failed      | 19040       | Indicates that enabling activity failed.           | 3                       |
| Monitor Activity Attempted  | 19041       | Indicates that monitoring activity was attempted.  | 1                       |
| Monitor Activity Succeeded  | 19042       | Indicates that monitoring activity was successful. | 1                       |
| Monitor Activity Failed     | 19043       | Indicates that monitoring activity failed.         | 3                       |
| Restore Activity Attempted  | 19044       | Indicates that restoring activity was attempted.   | 1                       |
| Restore Activity Succeeded  | 19045       | Indicates that restoring activity was successful.  | 1                       |
| Restore Activity Failed     | 19046       | Indicates that restoring activity failed.          | 3                       |
| Start Activity Attempted    | 19047       | Indicates that starting activity was attempted.    | 1                       |
| Start Activity Succeeded    | 19048       | Indicates that starting activity was successful.   | 1                       |
| Start Activity Failed       | 19049       | Indicates that starting activity failed.           | 3                       |
| Stop Activity Attempted     | 19050       | Indicates that stopping activity was attempted.    | 1                       |
| Stop Activity Succeeded     | 19051       | Indicates that stopping activity was successful.   | 1                       |
| Stop Activity Failed        | 19052       | Indicates that stopping activity failed.           | 3                       |
| Undeploy Activity Attempted | 19053       | Indicates that undeploy activity was attempted.    | 1                       |
| Undeploy Activity Succeeded | 19054       | Indicates that undeploy activity was successful.   | 1                       |
| Undeploy Activity Failed    | 19055       | Indicates that undeploy activity failed.           | 3                       |
| Receive Activity Attempted  | 19056       | Indicates that receiving activity was attempted.   | 1                       |
| Receive Activity Succeeded  | 19057       | Indicates that receiving activity was successful.  | 1                       |
| Receive Activity Failed     | 19058       | Indicates that receiving activity failed           | 3                       |



| <i>Table 56. Low-level categories and severity levels for the audit category (continued)</i> |                    |                                                 |                                |
|----------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                              | <b>Category ID</b> | <b>Description</b>                              | <b>Severity level (0 - 10)</b> |
| Send Activity Attempted                                                                      | 19059              | Indicates that sending activity was attempted.  | 1                              |
| Send Activity Succeeded                                                                      | 19060              | Indicates that sending activity was successful. | 1                              |
| Send Activity Failed                                                                         | 19061              | Indicates that sending activity failed.         | 3                              |

## Control

The control category contains events that are related to your hardware system.

The following table describes the low-level event categories and associated severity levels for the control category.

| <i>Table 57. Low-level categories and severity levels for the control category</i> |                    |                                                      |                                |
|------------------------------------------------------------------------------------|--------------------|------------------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                    | <b>Category ID</b> | <b>Description</b>                                   | <b>Severity level (0 - 10)</b> |
| Device Read                                                                        | 22001              | Indicates that a device was read.                    | 1                              |
| Device Communication                                                               | 22002              | Indicates communication with a device.               | 1                              |
| Device Audit                                                                       | 22003              | Indicates that a device audit occurred.              | 1                              |
| Device Event                                                                       | 22004              | Indicates that a device event occurred.              | 1                              |
| Device Ping                                                                        | 22005              | Indicates that a ping action to a device occurred.   | 1                              |
| Device Configuration                                                               | 22006              | Indicates that a device was configured.              | 1                              |
| Device Registration                                                                | 22007              | Indicates that a device was registered.              | 1                              |
| Device Route                                                                       | 22008              | Indicates that a device route action occurred.       | 1                              |
| Device Import                                                                      | 22009              | Indicates that a device import occurred.             | 1                              |
| Device Information                                                                 | 22010              | Indicates that a device information action occurred. | 1                              |
| Device Warning                                                                     | 22011              | Indicates that a warning was generated on a device.  | 1                              |

Table 57. Low-level categories and severity levels for the control category (continued)

| Low-level event category | Category ID | Description                                                  | Severity level (0 - 10) |
|--------------------------|-------------|--------------------------------------------------------------|-------------------------|
| Device Error             | 22012       | Indicates that an error was generated on a device.           | 1                       |
| Relay Event              | 22013       | Indicates a relay event.                                     | 1                       |
| NIC Event                | 22014       | Indicates a Network Interface Card (NIC) event.              | 1                       |
| UIQ Event                | 22015       | Indicates an event on a mobile device.                       | 1                       |
| IMU Event                | 22016       | Indicates an event on an Integrated Management Unit (IMU).   | 1                       |
| Billing Event            | 22017       | Indicates a billing event.                                   | 1                       |
| DBMS Event               | 22018       | Indicates an event on the Database Management System (DBMS). | 1                       |
| Import Event             | 22019       | Indicates that an import occurred.                           | 1                       |
| Location Import          | 22020       | Indicates that a location import occurred.                   | 1                       |
| Route Import             | 22021       | Indicates that a route import occurred.                      | 1                       |
| Export Event             | 22022       | Indicates that an export occurred.                           | 1                       |
| Remote Signaling         | 22023       | Indicates remote signaling.                                  | 1                       |
| Gateway Status           | 22024       | Indicates gateway status.                                    | 1                       |
| Job Event                | 22025       | Indicates that a job occurred.                               | 1                       |
| Security Event           | 22026       | Indicates that a security event occurred.                    | 1                       |
| Device Tamper Detection  | 22027       | Indicates that the system detected a tamper action.          | 1                       |
| Time Event               | 22028       | Indicates that a time event occurred.                        | 1                       |
| Suspicious Behavior      | 22029       | Indicates that suspicious behavior occurred.                 | 1                       |

| <i>Table 57. Low-level categories and severity levels for the control category (continued)</i> |                    |                                              |                                |
|------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                                | <b>Category ID</b> | <b>Description</b>                           | <b>Severity level (0 - 10)</b> |
| Power Outage                                                                                   | 22030              | Indicates that a power outage occurred.      | 1                              |
| Power Restoration                                                                              | 22031              | Indicates that power was restored.           | 1                              |
| Heartbeat                                                                                      | 22032              | Indicates that a heartbeat ping occurred.    | 1                              |
| Remote Connection Event                                                                        | 22033              | Indicates a remote connection to the system. | 1                              |

## Asset Profiler

The asset profiler category contains events that are related to asset profiles.

The following table describes the low-level event categories and associated severity levels for the asset profiler category.

| <i>Table 58. Low-level categories and severity levels for the asset profiler category</i> |                    |                                          |                                |
|-------------------------------------------------------------------------------------------|--------------------|------------------------------------------|--------------------------------|
| <b>Low-level event category</b>                                                           | <b>Category ID</b> | <b>Description</b>                       | <b>Severity level (0 - 10)</b> |
| Asset Created                                                                             | 23001              | Indicates that an asset was created.     | 1                              |
| Asset Updated                                                                             | 23002              | Indicates that an asset was updated.     | 1                              |
| Asset Observed                                                                            | 23003              | Indicates that an asset was observed.    | 1                              |
| Asset Moved                                                                               | 23004              | Indicates that an asset was moved.       | 1                              |
| Asset Deleted                                                                             | 23005              | Indicates that an asset was deleted.     | 1                              |
| Asset Hostname Cleaned                                                                    | 23006              | Indicates that a host name was cleaned.  | 1                              |
| Asset Hostname Created                                                                    | 23007              | Indicates that a host name was created.  | 1                              |
| Asset Hostname Updated                                                                    | 23008              | Indicates that a host name was updated.  | 1                              |
| Asset Hostname Observed                                                                   | 23009              | Indicates that a host name was observed. | 1                              |
| Asset Hostname Moved                                                                      | 23010              | Indicates that a host name was moved.    | 1                              |
| Asset Hostname Deleted                                                                    | 23011              | Indicates that a host name was deleted.  | 1                              |
| Asset Port Cleaned                                                                        | 23012              | Indicates that a port was cleaned.       | 1                              |

Table 58. Low-level categories and severity levels for the asset profiler category (continued)

| Low-level event category     | Category ID | Description                                           | Severity level (0 - 10) |
|------------------------------|-------------|-------------------------------------------------------|-------------------------|
| Asset Port Created           | 23013       | Indicates that a port was created.                    | 1                       |
| Asset Port Updated           | 23014       | Indicates that a port was updated.                    | 1                       |
| Asset Port Observed          | 23015       | Indicates that a port was observed.                   | 1                       |
| Asset Port Moved             | 23016       | Indicates that a port was moved.                      | 1                       |
| Asset Port Deleted           | 23017       | Indicates that a port was deleted.                    | 1                       |
| Asset Vuln Instance Cleaned  | 23018       | Indicates that a vulnerability instance was cleaned.  | 1                       |
| Asset Vuln Instance Created  | 23019       | Indicates that a vulnerability instance was created.  | 1                       |
| Asset Vuln Instance Updated  | 23020       | Indicates that a vulnerability instance was updated.  | 1                       |
| Asset Vuln Instance Observed | 23021       | Indicates that a vulnerability instance was observed. | 1                       |
| Asset Vuln Instance Moved    | 23022       | Indicates that a vulnerability instance was moved.    | 1                       |
| Asset Vuln Instance Deleted  | 23023       | Indicates that a vulnerability instance was deleted.  | 1                       |
| Asset OS Cleaned             | 23024       | Indicates that an operating system was cleaned.       | 1                       |
| Asset OS Created             | 23025       | Indicates that an operating system was created.       | 1                       |
| Asset OS Updated             | 23026       | Indicates that an operating system was updated.       | 1                       |
| Asset OS Observed            | 23027       | Indicates that an operating system was observed.      | 1                       |
| Asset OS Moved               | 23028       | Indicates that an operating system was moved.         | 1                       |

Table 58. Low-level categories and severity levels for the asset profiler category (continued)

| Low-level event category  | Category ID | Description                                     | Severity level (0 - 10) |
|---------------------------|-------------|-------------------------------------------------|-------------------------|
| Asset OS Deleted          | 23029       | Indicates that an operating system was deleted. | 1                       |
| Asset Property Cleaned    | 23030       | Indicates that a property was cleaned.          | 1                       |
| Asset Property Created    | 23031       | Indicates that a property was created.          | 1                       |
| Asset Property Updated    | 23032       | Indicates that a property was updated.          | 1                       |
| Asset Property Observed   | 23033       | Indicates that a property was observed.         | 1                       |
| Asset Property Moved      | 23034       | Indicates that a property was moved.            | 1                       |
| Asset Property Deleted    | 23035       | Indicates that a property was moved.            | 1                       |
| Asset IP Address Cleaned  | 23036       | Indicates that an IP address was cleaned.       | 1                       |
| Asset IP Address Created  | 23037       | Indicates that an IP address was created.       | 1                       |
| Asset IP Address Updated  | 23038       | Indicates that an IP address was updated.       | 1                       |
| Asset IP Address Observed | 23039       | Indicates that an IP address was observed.      | 1                       |
| Asset IP Address Moved    | 23040       | Indicates that an IP address was moved.         | 1                       |
| Asset IP Address Deleted  | 23041       | Indicates that an IP address was deleted.       | 1                       |
| Asset Interface Cleaned   | 23042       | Indicates that an interface was cleaned.        | 1                       |
| Asset Interface Created   | 23043       | Indicates that an interface was created.        | 1                       |
| Asset Interface Updated   | 23044       | Indicates that an interface was updated.        | 1                       |
| Asset Interface Observed  | 23045       | Indicates that an interface was observed.       | 1                       |
| Asset Interface Moved     | 23046       | Indicates that an interface was moved.          | 1                       |
| Asset Interface Merged    | 23047       | Indicates that an interface was merged.         | 1                       |
| Asset Interface Deleted   | 23048       | Indicates that an interface was deleted.        | 1                       |

*Table 58. Low-level categories and severity levels for the asset profiler category (continued)*

| <b>Low-level event category</b>    | <b>Category ID</b> | <b>Description</b>                                 | <b>Severity level (0 - 10)</b> |
|------------------------------------|--------------------|----------------------------------------------------|--------------------------------|
| Asset User Cleaned                 | 23049              | Indicates that a user was cleaned.                 | 1                              |
| Asset User Observed                | 23050              | Indicates that a user was observed.                | 1                              |
| Asset User Moved                   | 23051              | Indicates that a user was moved.                   | 1                              |
| Asset User Deleted                 | 23052              | Indicates that a user was deleted.                 | 1                              |
| Asset Scanned Policy Cleaned       | 23053              | Indicates that a scanned policy was cleaned.       | 1                              |
| Asset Scanned Policy Observed      | 23054              | Indicates that a scanned policy was observed.      | 1                              |
| Asset Scanned Policy Moved         | 23055              | Indicates that a scanned policy was moved.         | 1                              |
| Asset Scanned Policy Deleted       | 23056              | Indicates that a scanned policy was deleted.       | 1                              |
| Asset Windows Application Cleaned  | 23057              | Indicates that a Windows application was cleaned.  | 1                              |
| Asset Windows Application Observed | 23058              | Indicates that a Windows application was observed. | 1                              |
| Asset Windows Application Moved    | 23059              | Indicates that a Windows application was moved.    | 1                              |
| Asset Windows Application Deleted  | 23060              | Indicates that a Windows application was deleted.  | 1                              |
| Asset Scanned Service Cleaned      | 23061              | Indicates that a scanned service was cleaned.      | 1                              |
| Asset Scanned Service Observed     | 23062              | Indicates that a scanned service was observed.     | 1                              |
| Asset Scanned Service Moved        | 23063              | Indicates that a scanned service was moved.        | 1                              |
| Asset Scanned Service Deleted      | 23064              | Indicates that a scanned service was deleted.      | 1                              |
| Asset Windows Patch Cleaned        | 23065              | Indicates that a Windows patch was cleaned.        | 1                              |
| Asset Windows Patch Observed       | 23066              | Indicates that a Windows patch was observed.       | 1                              |

Table 58. Low-level categories and severity levels for the asset profiler category (continued)

| Low-level event category          | Category ID | Description                                       | Severity level (0 - 10) |
|-----------------------------------|-------------|---------------------------------------------------|-------------------------|
| Asset Windows Patch Moved         | 23067       | Indicates that a Windows patch was moved.         | 1                       |
| Asset Windows Patch Deleted       | 23068       | Indicates that a Windows patch was deleted.       | 1                       |
| Asset UNIX Patch Cleaned          | 23069       | Indicates that a UNIX patch was cleaned.          | 1                       |
| Asset UNIX Patch Observed         | 23070       | Indicates that a UNIX patch was observed.         | 1                       |
| Asset UNIX Patch Moved            | 23071       | Indicates that a UNIX patch was moved.            | 1                       |
| Asset UNIX Patch Deleted          | 23072       | Indicates that a UNIX patch was deleted.          | 1                       |
| Asset Patch Scan Cleaned          | 23073       | Indicates that a patch scan was cleaned.          | 1                       |
| Asset Patch Scan Created          | 23074       | Indicates that a patch scan was created.          | 1                       |
| Asset Patch Scan Moved            | 23075       | Indicates that a patch scan was moved.            | 1                       |
| Asset Patch Scan Deleted          | 23076       | Indicates that a patch scan was deleted.          | 1                       |
| Asset Port Scan Cleaned           | 23077       | Indicates that a port scan was cleaned.           | 1                       |
| Asset Port Scan Created           | 23078       | Indicates that a port scan was cleaned.           | 1                       |
| Asset Port Scan Moved             | 23079       | Indicates that a patch scan was moved.            | 1                       |
| Asset Port Scan Deleted           | 23080       | Indicates that a patch scan was deleted.          | 1                       |
| Asset Client Application Cleaned  | 23081       | Indicates that a client application was cleaned.  | 1                       |
| Asset Client Application Observed | 23082       | Indicates that a client application was observed. | 1                       |
| Asset Client Application Moved    | 23083       | Indicates that a client application was moved.    | 1                       |
| Asset Client Application Deleted  | 23084       | Indicates that a client application was deleted.  | 1                       |
| Asset Patch Scan Observed         | 23085       | Indicates that a patch scan was observed.         | 1                       |

Table 58. Low-level categories and severity levels for the asset profiler category (continued)

| Low-level event category | Category ID | Description                                  | Severity level (0 - 10) |
|--------------------------|-------------|----------------------------------------------|-------------------------|
| Asset Port Scan Observed | 23086       | Indicates that a port scan was observed.     | 1                       |
| NetBIOS Group Created    | 23087       | Indicates that a NetBIOS group was created.  | 1                       |
| NetBIOS Group Updated    | 23088       | Indicates that a NetBIOS group was updated.  | 1                       |
| NetBIOS Group Observed   | 23089       | Indicates that a NetBIOS group was observed. | 1                       |
| NetBIOS Group Deleted    | 23090       | Indicates that a NetBIOS group was deleted.  | 1                       |
| NetBIOS Group Cleaned    | 23091       | Indicates that a NetBIOS group was cleaned.  | 1                       |
| NetBIOS Group Moved      | 23092       | Indicates that a NetBIOS group was moved.    | 1                       |

## Sense

The sense category contains events that are related to sense user behavior analytics.

The following table describes the low-level event categories and associated severity levels for the sense category.

Table 59.

| Low-level event category | Category ID | Description                              | Severity level (0 - 10) |
|--------------------------|-------------|------------------------------------------|-------------------------|
| User Behavior            | 24001       | Indicates the user's behavior.           | 5                       |
| User Geography           | 24002       | Indicates the user's geography.          | 5                       |
| User Time                | 24003       | Indicates the user's time.               | 5                       |
| User Access              | 24004       | Indicates the user's access.             | 5                       |
| User Privilege           | 24005       | Indicates the user's privilege.          | 5                       |
| User Risk                | 24006       | Indicates the user's risk.               | 5                       |
| Sense Offense            | 24007       | Indicates that a sense offense occurred. | 5                       |



| <i>Table 59. (continued)</i>    |                    |                                           |                                |
|---------------------------------|--------------------|-------------------------------------------|--------------------------------|
| <b>Low-level event category</b> | <b>Category ID</b> | <b>Description</b>                        | <b>Severity level (0 - 10)</b> |
| Resource Risk                   | 24008              | Indicates the resources that are at risk. | 5                              |



---

## Chapter 21. Common ports and servers used by QRadar

IBM QRadar requires that certain ports are ready to receive information from QRadar components and external infrastructure. To ensure that QRadar is using the most recent security information, it also requires access to public servers and RSS feeds.

### SSH communication on port 22

All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely. These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. IBM QRadar QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

### Open ports that are not required by QRadar

You might find additional open ports in the following situations:

- When you install QRadar on your own hardware, you may see open ports that are used by services, daemons, and programs included in Red Hat Enterprise Linux.
- When you mount or export a network file share, you might see dynamically assigned ports that are required for RPC services, such as `rpc.mountd` and `rpc.rquotad`.

#### Related concepts

[Capabilities in your IBM QRadar product](#)

---

## QRadar port usage

Review the list of common ports that IBM QRadar services and components use to communicate across the network. You can use the port list to determine which ports must be open in your network. For example, you can determine which ports must be open for the QRadar Console to communicate with remote event processors.

### WinCollect remote polling

WinCollect agents that remotely poll other Microsoft Windows operating systems might require additional port assignments.

For more information, see the IBM QRadar WinCollect *User Guide*.

### QRadar listening ports

The following table shows the QRadar ports that are open in a LISTEN state. The LISTEN ports are valid only when iptables is enabled on your system. Unless otherwise noted, information about the assigned port number applies to all QRadar products.

Table 60. Listening ports that are used by QRadar services and components

| Port                                                          | Description                  | Protocol | Direction                                                                                                                                                                                                                                                                                                                                                                 | Requirement                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------|------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22                                                            | SSH                          | TCP      | Bidirectional from the QRadar Console to all other components.                                                                                                                                                                                                                                                                                                            | Remote management access.<br><br>Adding a remote system as a managed host.<br><br>Log source protocols to retrieve files from external devices, for example the log file protocol.<br><br>Users who use the command-line interface to communicate from desktops to the Console.<br><br>High-availability (HA).                     |
| 25                                                            | SMTP                         | TCP      | From all managed hosts to the SMTP gateway.                                                                                                                                                                                                                                                                                                                               | Emails from QRadar to an SMTP gateway.<br><br>Delivery of error and warning email messages to an administrative email contact.                                                                                                                                                                                                     |
| 111                                                           | Port mapper                  | TCP/UDP  | Managed hosts (MH) that communicate with the QRadar Console.<br><br>Users that connect to the QRadar Console.                                                                                                                                                                                                                                                             | Remote Procedure Calls (RPC) for required services, such as Network File System (NFS).                                                                                                                                                                                                                                             |
| 123                                                           | Network Time Protocol (NTP)  | UDP      | Outbound from the QRadar Console to the NTP Server<br><br>Outbound from the MH to the QRadar Console                                                                                                                                                                                                                                                                      | Time synchronization via Chrony between:<br><ul style="list-style-type: none"><li>QRadar Console and NTP server</li><li>QRadar Managed Hosts and QRadar Console</li></ul>                                                                                                                                                          |
| 135 and dynamically allocated ports above 1024 for RPC calls. | DCOM                         | TCP      | Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.<br><br>Bidirectional traffic between QRadar Console components or IBM QRadar event collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events. | This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.<br><br><b>Note:</b> DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation. |
| 137                                                           | Windows NetBIOS name service | UDP      | Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.<br><br>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.     | This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.                                                                                                                                                                                                                          |

Table 60. Listening ports that are used by QRadar services and components (continued)

| Port | Description                      | Protocol | Direction                                                                                                                                                                                                                                                                                                                                                                    | Requirement                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 138  | Windows NetBIOS datagram service | UDP      | <p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p> | This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.                                                                                                                                                                                                                            |
| 139  | Windows NetBIOS session service  | TCP      | <p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use either Microsoft Security Event Log Protocol or Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p> | This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.                                                                                                                                                                                                                            |
| 162  | NetSNMP                          | UDP      | <p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>                                                                                                                                                                                                                                                      | UDP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.                                                                                                                                                                   |
| 199  | NetSNMP                          | TCP      | <p>QRadar managed hosts that connect to the QRadar Console.</p> <p>External log sources to QRadar Event Collectors.</p>                                                                                                                                                                                                                                                      | TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources. The port is open only when the SNMP agent is enabled.                                                                                                                                                                   |
| 427  | Service Location Protocol (SLP)  | UDP/TCP  |                                                                                                                                                                                                                                                                                                                                                                              | The Integrated Management Module uses the port to find services on a LAN.                                                                                                                                                                                                                                                            |
| 443  | Apache/HTTPS                     | TCP      | <p>Bidirectional traffic for secure communications from all products to the QRadar Console.</p> <p>Unidirectional traffic from the App Host to the QRadar Console.</p>                                                                                                                                                                                                       | <p>Configuration downloads to managed hosts from the QRadar Console.</p> <p>QRadar managed hosts that connect to the QRadar Console.</p> <p>Users to have log in access to QRadar.</p> <p>QRadar Console that manage and provide configuration updates for WinCollect agents.</p> <p>Apps that require access to the QRadar API.</p> |

Table 60. Listening ports that are used by QRadar services and components (continued)

| Port | Description                                                    | Protocol | Direction                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Requirement                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 445  | Microsoft Directory Service                                    | TCP      | <p>Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between QRadar Console components or QRadar Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events.</p> <p>Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.</p> | This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.                                                                                                                        |
| 514  | Syslog                                                         | UDP/TCP  | <p>External network appliances that provide TCP syslog events use bidirectional traffic.</p> <p>External network appliances that provide UDP syslog events use uni-directional traffic.</p> <p>Internal syslog traffic from QRadar hosts to the QRadar Console.</p>                                                                                                                                                                                                            | <p>External log sources to send event data to QRadar components.</p> <p>Syslog traffic includes WinCollect agents, event collectors, and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar.</p> |
| 762  | Network File System (NFS) mount daemon (mountd)                | TCP/UDP  | Connections between the QRadar Console and NFS server.                                                                                                                                                                                                                                                                                                                                                                                                                         | The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location.                                                                                                             |
| 1514 | Syslog-ng                                                      | TCP/UDP  | Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging.                                                                                                                                                                                                                                                                                                                                                | Internal logging port for syslog-ng.                                                                                                                                                                                             |
| 2049 | NFS                                                            | TCP      | Connections between the QRadar Console and NFS server.                                                                                                                                                                                                                                                                                                                                                                                                                         | The Network File System (NFS) protocol to share files or data between components.                                                                                                                                                |
| 2055 | NetFlow data                                                   | UDP      | From the management interface on the flow source (typically a router) to the IBM QRadar QFlow Collector.                                                                                                                                                                                                                                                                                                                                                                       | NetFlow datagram from components, such as routers.                                                                                                                                                                               |
| 2376 | Docker command port                                            | TCP      | Internal communications. This port is not available externally.                                                                                                                                                                                                                                                                                                                                                                                                                | Used to manage QRadar application framework resources.                                                                                                                                                                           |
| 3389 | Remote Desktop Protocol (RDP) and Ethernet over USB is enabled | TCP/UDP  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | If the Microsoft Windows operating system is configured to support RDP and Ethernet over USB, a user can initiate a session to the server over the management network. This means the default port for RDP, 3389 must be open.   |
| 3900 | Integrated Management Module remote presence port              | TCP/UDP  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Use this port to interact with the QRadar console through the Integrated Management Module.                                                                                                                                      |

Table 60. Listening ports that are used by QRadar services and components (continued)

| Port                                                                                                                        | Description                                                                                                                                                                               | Protocol | Direction                                                                                                                                            | Requirement                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4333                                                                                                                        | Redirect port                                                                                                                                                                             | TCP      |                                                                                                                                                      | This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution.                                                                                                                                                                          |
| 5000                                                                                                                        | Used to allow communication to the docker si-registry running on the Console. This allows all managed hosts to pull images from the Console that will be used to create local containers. | TCP      | Unidirectional from the QRadar managed host to the QRadar Console. The port is only opened on the Console. Managed hosts must pull from the Console. | Required for apps running on an App Host.                                                                                                                                                                                                                                                      |
| 5432                                                                                                                        | Postgres                                                                                                                                                                                  | TCP      | Communication for the managed host that is used to access the local database instance.                                                               | Required for provisioning managed hosts from the <b>Admin</b> tab.                                                                                                                                                                                                                             |
| 6514                                                                                                                        | Syslog                                                                                                                                                                                    | TCP      | External network appliances that provide encrypted TCP syslog events use bidirectional traffic.                                                      | External log sources to send encrypted event data to QRadar components.                                                                                                                                                                                                                        |
| 7676, 7677, and four randomly bound ports above 32000.                                                                      | Messaging connections (IMQ)                                                                                                                                                               | TCP      | Message queue communications between components on a managed host.                                                                                   | Message queue broker for communications between components on a managed host.<br><br><b>Note:</b> You must permit access to these ports from the QRadar console to unencrypted hosts.<br><br>Ports 7676 and 7677 are static TCP ports, and four extra connections are created on random ports. |
| 5791, 7700, 7777, 7778, 7779, 7780, 7781, 7782, 7783, 7787, 7788, 7790, 7791, 7792, 7793, 7794, 7795, 7799, 8989, and 8990. | JMX server ports                                                                                                                                                                          | TCP      | Internal communications. These ports are not available externally.                                                                                   | JMX server (Java™ Management Beans) monitoring for all internal QRadar processes to expose supportability metrics.<br><br>These ports are used by QRadar support.                                                                                                                              |
| 7789                                                                                                                        | HA Distributed Replicated Block Device                                                                                                                                                    | TCP/UDP  | Bidirectional between the secondary host and primary host in an HA cluster.                                                                          | Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations.                                                                                                                                                          |
| 7800                                                                                                                        | Apache Tomcat                                                                                                                                                                             | TCP      | From the Event Processor to the QRadar Console.                                                                                                      | Real-time (streaming) for events.                                                                                                                                                                                                                                                              |
| 7801                                                                                                                        | Apache Tomcat                                                                                                                                                                             | TCP      | From the Event Processor to the QRadar Console.                                                                                                      | Real-time (streaming) for flows.                                                                                                                                                                                                                                                               |
| 7803                                                                                                                        | Anomaly Detection Engine                                                                                                                                                                  | TCP      | From the Event Processor to the QRadar Console.                                                                                                      | Anomaly detection engine port.                                                                                                                                                                                                                                                                 |
| 7804                                                                                                                        | QRM Arc builder                                                                                                                                                                           | TCP      | Internal control communications between QRadar processes and ARC builder.                                                                            | This port is used for QRadar Risk Manager only. It is not available externally.                                                                                                                                                                                                                |
| 7805                                                                                                                        | Syslog tunnel communication                                                                                                                                                               | TCP      | Bidirectional between the QRadar Console and managed hosts                                                                                           | Used for encrypted communication between the console and managed hosts.                                                                                                                                                                                                                        |

Table 60. Listening ports that are used by QRadar services and components (continued)

| Port                                    | Description                              | Protocol | Direction                                                                                                           | Requirement                                                                                                                                                                                        |
|-----------------------------------------|------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8000                                    | Event Collection service (ECS)           | TCP      | From the Event Collector to the QRadar Console.                                                                     | Listening port for specific Event Collection Service (ECS).                                                                                                                                        |
| 8001                                    | SNMP daemon port                         | TCP      | External SNMP systems that request SNMP trap information from the QRadar Console.                                   | Listening port for external SNMP data requests.                                                                                                                                                    |
| 8005                                    | Apache Tomcat                            | TCP      | Internal communications. Not available externally.                                                                  | Open to control tomcat.<br><br>This port is bound and only accepts connections from the local host.                                                                                                |
| 8009                                    | Apache Tomcat                            | TCP      | From the HTTP daemon (HTTPd) process to Tomcat.                                                                     | Tomcat connector, where the request is used and proxied for the web service.                                                                                                                       |
| 8080                                    | Apache Tomcat                            | TCP      | From the HTTP daemon (HTTPd) process to Tomcat.                                                                     | Tomcat connector, where the request is used and proxied for the web service.                                                                                                                       |
| 8082                                    | Secure tunnel for QRadar Risk Manager    | TCP      | Bidirectional traffic between the QRadar Console and QRadar Risk Manager                                            | Required when encryption is used between QRadar Risk Manager and the QRadar Console.                                                                                                               |
| 8413                                    | WinCollect agents                        | TCP      | Bidirectional traffic between WinCollect agent and QRadar Console.                                                  | This traffic is generated by the WinCollect agent and communication is encrypted. It is required to provide configuration updates to the WinCollect agent and to use WinCollect in connected mode. |
| 8844                                    | Apache Tomcat                            | TCP      | Unidirectional from the QRadar Console to the appliance that is running the QRadar Vulnerability Manager processor. | Used by Apache Tomcat to read RSS feeds from the host that is running the QRadar Vulnerability Manager processor.                                                                                  |
| 9000                                    | Conman                                   | TCP      | Unidirectional from the QRadar Console to a QRadar App Host.                                                        | Used with an App Host. It allows the Console to deploy apps to an App Host and to manage those apps.                                                                                               |
| 9090                                    | XForce IP Reputation database and server | TCP      | Internal communications. Not available externally.                                                                  | Communications between QRadar processes and the XForce Reputation IP database.                                                                                                                     |
| 9381                                    | Certificate files download               | TCP      | Unidirectional from QRadar managed host or external network to QRadar Console                                       | Downloading QRadar CA certificate and CRL files, which can be used to validate QRadar generated certificates.                                                                                      |
| 9381                                    | localca-server                           | TCP      | Bidirectional between QRadar components.                                                                            | Used to hold QRadar local root and intermediate certificates, as well as associated CRLs.                                                                                                          |
| 9393, 9394                              | vault-qrd                                | TCP      | Internal communications. Not available externally.                                                                  | Used to hold secrets and allow secure access to them to services.                                                                                                                                  |
| 9913 plus one dynamically assigned port | Web application container                | TCP      | Bidirectional Java Remote Method Invocation (RMI) communication between Java Virtual Machines                       | When the web application is registered, one additional port is dynamically assigned.                                                                                                               |



Table 60. Listening ports that are used by QRadar services and components (continued)

| Port         | Description                                       | Protocol | Direction                                                                                            | Requirement                                                                                                                                                                                                                                         |
|--------------|---------------------------------------------------|----------|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9995         | NetFlow data                                      | UDP      | From the management interface on the flow source (typically a router) to the QRadar QFlow Collector. | NetFlow datagram from components, such as routers.                                                                                                                                                                                                  |
| 9999         | IBM QRadar Vulnerability Manager processor        | TCP      | Unidirectional from the scanner to the appliance running the QRadar Vulnerability Manager processor  | Used for QRadar Vulnerability Manager (QVM) command information. The QRadar Console connects to this port on the host that is running the QRadar Vulnerability Manager processor. This port is only used when QVM is enabled.                       |
| 10000        | QRadar web-based, system administration interface | TCP/UDP  | User desktop systems to all QRadar hosts.                                                            | In QRadar V7.2.5 and earlier, this port is used for server changes, such as the hosts root password and firewall access.<br><br>Port 10000 is disabled in V7.2.6.                                                                                   |
| 10101, 10102 | Heartbeat command                                 | TCP      | Bidirectional traffic between the primary and secondary HA nodes.                                    | Required to ensure that the HA nodes are still active.                                                                                                                                                                                              |
| 12500        | Socat binary                                      | TCP      | Outbound from MH to the QRadar Console                                                               | Port used for tunneling chrony udp requests over tcp when QRadar Console or MH is encrypted                                                                                                                                                         |
| 14433        | traefik                                           | TCP      | Bidirectional between QRadar components.                                                             | Required for app services discovery.                                                                                                                                                                                                                |
| 15432        |                                                   |          |                                                                                                      | Required to be open for internal communication between QRM and QRadar.                                                                                                                                                                              |
| 15433        | Postgres                                          | TCP      | Communication for the managed host that is used to access the local database instance.               | Used for QRadar Vulnerability Manager (QVM) configuration and storage. This port is only used when QVM is enabled.                                                                                                                                  |
| 15434        |                                                   |          |                                                                                                      | Required to be open for internal communication between Forensics and QRadar.                                                                                                                                                                        |
| 20000-23000  | SSH Tunnel                                        | TCP      | Bidirectional from the QRadar Console to all other encrypted managed hosts.                          | Local listening point for SSH tunnels used for Java Message Service (JMS) communication with encrypted managed hosts. Used to perform long-running asynchronous tasks, such as updating networking configuration via System and License Management. |
| 23111        | SOAP web server                                   | TCP      |                                                                                                      | SOAP web server port for the Event Collection Service (ECS).                                                                                                                                                                                        |
| 23333        | Emulex Fibre Channel                              | TCP      | User desktop systems that connect to QRadar appliances with a Fibre Channel card.                    | Emulex Fibre Channel HBA anywhere Remote Management service (elxmgmt).                                                                                                                                                                              |

Table 60. Listening ports that are used by QRadar services and components (continued)

| Port        | Description                             | Protocol | Direction                                                                           | Requirement                                                                                                                                                                                                                                                                                      |
|-------------|-----------------------------------------|----------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 32000       | Normalized flow forwarding              | TCP      | Bidirectional between QRadar components.                                            | Normalized flow data that is communicated from an off-site source or between QRadar QFlow Collectors.                                                                                                                                                                                            |
| 32004       | Normalized event forwarding             | TCP      | Bidirectional between QRadar components.                                            | Normalized event data that is communicated from an off-site source or between QRadar Event Collectors.                                                                                                                                                                                           |
| 32005       | Data flow                               | TCP      | Bidirectional between QRadar components.                                            | Data flow communication port between QRadar Event Collectors when on separate managed hosts.                                                                                                                                                                                                     |
| 32006       | Ariel queries                           | TCP      | Bidirectional between QRadar components.                                            | Communication port between the Ariel proxy server and the Ariel query server.                                                                                                                                                                                                                    |
| 32007       | Offense data                            | TCP      | Bidirectional between QRadar components.                                            | Events and flows contributing to an offense or involved in global correlation.                                                                                                                                                                                                                   |
| 32009       | Identity data                           | TCP      | Bidirectional between QRadar components.                                            | Identity data that is communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS).                                                                                                                                                           |
| 32010       | Flow listening source port              | TCP      | Bidirectional between QRadar components.                                            | Flow listening port to collect data from QRadar QFlow Collectors.                                                                                                                                                                                                                                |
| 32011       | Ariel listening port                    | TCP      | Bidirectional between QRadar components.                                            | Ariel listening port for database searches, progress information, and other associated commands.                                                                                                                                                                                                 |
| 32000-33999 | Data flow (flows, events, flow context) | TCP      | Bidirectional between QRadar components.                                            | Data flows, such as events, flows, flow context, event search queries, and Docker proxy.                                                                                                                                                                                                         |
| 40799       | PCAP data                               | UDP      | From Juniper Networks SRX Series appliances to QRadar.                              | Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances.<br><br><b>Note:</b> The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation. |
| ICMP        | ICMP                                    |          | Bidirectional traffic between the secondary host and primary host in an HA cluster. | Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP).                                                                                                                                                   |

## QRadar public servers

To provide you with the most current security information, IBM QRadar requires access to a number of public servers and RSS feeds.

### Public servers

| <i>Table 61. Public servers that QRadar must access.</i> This table lists descriptions for the IP addresses or host names that QRadar accesses. |                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP address or hostname                                                                                                                          | Description                                                                                                                                                                                                                                                         |
| 194.153.113.31                                                                                                                                  | IBM QRadar Vulnerability Manager DMZ scanner                                                                                                                                                                                                                        |
| 194.153.113.32                                                                                                                                  | QRadar Vulnerability Manager DMZ scanner                                                                                                                                                                                                                            |
| auto-update.qradar.ibmcloud.com/                                                                                                                | QRadar auto-update servers.<br>For more information about auto-update servers, see QRadar: Important auto update server changes for administrators ( <a href="https://www.ibm.com/support/pages/node/6244622">https://www.ibm.com/support/pages/node/6244622</a> ). |
| update.xforce-security.com                                                                                                                      | X-Force Threat Feed update server                                                                                                                                                                                                                                   |
| license.xforce-security.com                                                                                                                     | X-Force Threat Feed licensing server                                                                                                                                                                                                                                |

### RSS feeds for QRadar products

| <i>Table 62. RSS feeds .</i> The following list describes the requirements for RSS feeds that QRadar uses. Copy URLs into a text editor and remove page breaks before pasting into a browser. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Title                                                                                                                                                                                         | URL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Requirements                                           |
| Security Intelligence                                                                                                                                                                         | <a href="http://feeds.feedburner.com/SecurityIntelligence">http://feeds.feedburner.com/SecurityIntelligence</a>                                                                                                                                                                                                                                                                                                                                                                                 | QRadar and an Internet connection                      |
| Security Intelligence Vulns / Threats                                                                                                                                                         | <a href="http://securityintelligence.com/topics/vulnerabilities-threats/feed">http://securityintelligence.com/topics/vulnerabilities-threats/feed</a>                                                                                                                                                                                                                                                                                                                                           | QRadar and an Internet connection                      |
| IBM My Notifications                                                                                                                                                                          | <a href="http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgoth&amp;feeder.maxfeed=25">http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid=feeder.create_feed&amp;feeder.feedtype=RSS&amp;feeder.uid=270006EH0R&amp;feeder.subscrid=S14b5f284d32&amp;feeder.subdefkey=swgoth&amp;feeder.maxfeed=25</a> | QRadar and an Internet connection                      |
| Security News                                                                                                                                                                                 | <a href="http://IP_address_of_QVM_processor:8844/rss/research/news.rss">http://IP_address_of_QVM_processor:8844/rss/research/news.rss</a>                                                                                                                                                                                                                                                                                                                                                       | IBM QRadar Vulnerability Manager processor is deployed |
| Security Advisories                                                                                                                                                                           | <a href="http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss">http://IP_address_of_QVM_processor:8844/rss/research/advisories.rss</a>                                                                                                                                                                                                                                                                                                                                           | QRadar Vulnerability Manager processor is deployed     |
| Latest Published Vulnerabilities                                                                                                                                                              | <a href="http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss">http://IP_address_of_QVM_processor:8844/rss/research/vulnerabilities.rss</a>                                                                                                                                                                                                                                                                                                                                 | QRadar Vulnerability Manager processor deployed        |

*Table 62. RSS feeds . The following list describes the requirements for RSS feeds that QRadar uses. Copy URLs into a text editor and remove page breaks before pasting into a browser. (continued)*

| <b>Title</b>      | <b>URL</b>                                                                              | <b>Requirements</b>                                |
|-------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------|
| Scans Completed   | <code>http://IP_address_of_QVM_processor:8844/rss/scanresults/completedScans.rss</code> | QRadar Vulnerability Manager processor is deployed |
| Scans In Progress | <code>http://IP_address_of_QVM_processor:8844/rss/scanresults/runningScans.rss</code>   | QRadar Vulnerability Manager processor is deployed |

---

## Chapter 22. RESTful API

The representational state transfer (REST) application programming interface (API) is useful when you want to integrate IBM QRadar with other solutions. You can perform actions on the QRadar Console by sending HTTPS requests to specific endpoints (URLs) on the QRadar Console.

Each endpoint contains the URL of the resource that you want to access and the action that you want to complete on that resource. The action is indicated by the HTTP method of the request: GET, POST, PUT, or DELETE. For more information about the parameters and responses for each endpoint, see the *IBM QRadar API Guide*.

### QRadar API forum and code samples

The API forum provides more information about the REST API, including the answers to frequently asked questions and annotated code samples that you can use in a test environment. For more information, see the [API forum](https://ibm.biz/qradarforums) (<https://ibm.biz/qradarforums>).

---

## Accessing the interactive API documentation page

Use the interactive API documentation page to access technical details for the RESTful APIs and experiment with making API requests to your server.

### About this task

The API documentation user interface provides descriptions and the ability to use the following REST API interfaces:

| Table 63. REST API interfaces |                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| REST API                      | Description                                                                                                                                        |
| /api/analytics                | Create, update, and remove custom actions for rules.                                                                                               |
| /api/ariel                    | View event and flow properties, create event and flow searches, and manage searches.                                                               |
| /api/asset_model              | Returns a list of all assets in the model. You can also list all available asset property types and saved searches, and update an asset.           |
| /api/auth                     | Log out and invalidate the current session.                                                                                                        |
| /api/config                   | View and manage tenants, domains, and QRadar extensions.                                                                                           |
| /api/data_classification      | View all high and low-level categories, QRadar Identifier (QID) records, and event mappings. You can also create or edit QID records and mappings. |
| /api/forensics                | Manage capture recoveries and cases.                                                                                                               |
| /api/gui_app_framework        | Install and manage applications that are created by using the GUI Application Framework Software Development Kit.                                  |
| /api/help                     | Returns a list of API capabilities.                                                                                                                |

Table 63. REST API interfaces (continued)

| REST API            | Description                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /api/qrm            | Manage QRM saved search groups, question groups, simulation groups, topology saved search groups, and model groups.                                                                               |
| /api/qvm            | Retrieves assets, vulnerabilities, networks, open services, networks, and filters. You can also create or update remediation tickets.                                                             |
| /api/reference_data | View and manage reference data collections.                                                                                                                                                       |
| /api/scanner        | View, create, or start a remote scan that is related to a scan profile.                                                                                                                           |
| /api/services       | Perform tasks such as WHOIS lookups, port scan lookups, DNS lookups, and DIG lookups. You can also retrieve geolocation data for an IP or set of IP addresses.                                    |
| /api/siem           | View, update, and close offenses. You can also add notes and manage offense closing reasons.                                                                                                      |
| /api/staged_config  | Retrieve staged configuration for users, hosts, notifications, remote networks, and remote services. You can also initiate or see the state of a deploy action, and update and delete Yara rules. |
| /api/system         | Manage server hosts, network interfaces, and firewall rules.                                                                                                                                      |

## Procedure

1. To access the interactive API documentation interface, enter the following URL in your web browser:  
`https://ConsoleIPAddress/api_doc/`.
2. Select the API version that you want to use from the list.
3. Go to the endpoint that you want to access.
4. Read the endpoint documentation and complete the request parameters.
5. Click **Try it out** to send the API request to your console and receive a properly formatted HTTPS response.

**Note:** When you click **Try it out**, the action is performed on the QRadar system. Not all actions can be reversed, for example, you cannot reopen an offense after you close it.

6. Review and gather the information that you need to integrate with QRadar.

## Notices

---

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

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 grant 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.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 document 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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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 actual people or business enterprises is entirely coincidental.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://ibm.com)® are trademarks or registered trademarks 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 [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Linux is a registered trademark of Linus Torvalds 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.



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

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

## 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.

## IBM Online Privacy Statement

---

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.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

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> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details/> the section entitled "Cookies, Web Beacons and Other Technologies".

## General Data Protection Regulation

---

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing

advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: <https://ibm.com/gdpr>

# Glossary

---

This glossary provides terms and definitions for the IBM QRadar SIEM software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the [IBM Terminology website](#) (opens in new window).

## A

---

### **accumulator**

A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

### **active system**

In a high-availability (HA) cluster, the system that has all of its services running.

### **Address Resolution Protocol (ARP)**

A protocol that dynamically maps an IP address to a network adapter address in a local area network.

### **administrative share**

A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

### **anomaly**

A deviation from the expected behavior of the network.

### **application signature**

A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

### **ARP**

See [Address Resolution Protocol](#).

### **ARP Redirect**

An ARP method for notifying the host if a problem exists on a network.

### **ASN**

See [autonomous system number](#).

### **asset**

A manageable object that is either deployed or intended to be deployed in an operational environment.

### **autonomous system number (ASN)**

In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

## B

---

### **behavior**

The observable effects of an operation or event, including its results.

### **bonded interface**

See [link aggregation](#).

### **burst**

A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

## C

---

### **CIDR**

See [Classless Inter-Domain Routing](#).

### **Classless Inter-Domain Routing (CIDR)**

A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

### **client**

A software program or computer that requests services from a server.

### **cluster virtual IP address**

An IP address that is shared between the primary or secondary host and the HA cluster.

### **coalescing interval**

The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

### **Common Vulnerability Scoring System (CVSS)**

A scoring system by which the severity of a vulnerability is measured.

### **console**

A display station from which an operator can control and observe the system operation.

### **content capture**

A process that captures a configurable amount of payload and then stores the data in a flow log.

### **credential**

A set of information that grants a user or process certain access rights.

### **credibility**

A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

### **CVSS**

See [Common Vulnerability Scoring System](#).

## D

---

### **database leaf object**

A terminal object or node in a database hierarchy.

### **datapoint**

A calculated value of a metric at a point in time.

### **Device Support Module (DSM)**

A configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output.

### **DHCP**

See [Dynamic Host Configuration Protocol](#).

### **DNS**

See [Domain Name System](#).

### **Domain Name System (DNS)**

The distributed database system that maps domain names to IP addresses.

### **DSM**

See [Device Support Module](#).

### **duplicate flow**

Multiple instances of the same data transmission received from different flow sources.

## **Dynamic Host Configuration Protocol (DHCP)**

A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

## **E**

---

### **encryption**

In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

### **endpoint**

The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

### **external scanning appliance**

A machine that is connected to the network to gather vulnerability information about assets in the network.

## **F**

---

### **false positive**

An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

### **flow**

A single transmission of data passing over a link during a conversation.

### **flow log**

A collection of flow records.

### **flow sources**

The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

### **forwarding destination**

One or more vendor systems that receive raw and normalized data from log sources and flow sources.

### **FQDN**

See [fully qualified domain name](#).

### **FQNN**

See [fully qualified network name](#).

### **fully qualified domain name (FQDN)**

In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is `rchland.vnet.ibm.com`.

### **fully qualified network name (FQNN)**

In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is `CompanyA.Department.Marketing`.

## **G**

---

### **gateway**

A device or program used to connect networks or systems with different network architectures.

## **H**

---

### **HA**

See [high availability](#).

### **HA cluster**

A high-availability configuration consisting of a primary server and one secondary server.

**Hash-Based Message Authentication Code (HMAC)**

A cryptographic code that uses a cryptic hash function and a secret key.

**high availability (HA)**

Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

**HMAC**

See [Hash-Based Message Authentication Code](#).

**host context**

A service that monitors components to ensure that each component is operating as expected.

## I

---

**ICMP**

See [Internet Control Message Protocol](#).

**identity**

A collection of attributes from a data source that represent a person, organization, place, or item.

**IDS**

See [intrusion detection system](#).

**Internet Control Message Protocol (ICMP)**

An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

**Internet Protocol (IP)**

A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also [Transmission Control Protocol](#).

**Internet service provider (ISP)**

An organization that provides access to the Internet.

**intrusion detection system (IDS)**

Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

**intrusion prevention system (IPS)**

A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

**IP**

See [Internet Protocol](#).

**IP multicast**

Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

**IPS**

See [intrusion prevention system](#).

**ISP**

See [Internet service provider](#).

## K

---

**key file**

In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

## L

---

**L2L**

See [Local To Local](#).

**L2R**

See [Local To Remote](#).

**LAN**

See [local area network](#).

**LDAP**

See [Lightweight Directory Access Protocol](#).

**leaf**

In a tree, an entry or node that has no children.

**Lightweight Directory Access Protocol (LDAP)**

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

**link aggregation**

The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

**live scan**

A vulnerability scan that generates report data from the scan results based on the session name.

**local area network (LAN)**

A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

**Local To Local (L2L)**

Pertaining to the internal traffic from one local network to another local network.

**Local To Remote (L2R)**

Pertaining to the internal traffic from one local network to another remote network.

**log source**

Either the security equipment or the network equipment from which an event log originates.

**log source extension**

An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

## M

---

**Magistrate**

An internal component that analyzes network traffic and security events against defined custom rules.

**magnitude**

A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

## N

---

**NAT**

See [network address translation](#).

**NetFlow**

A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

**network address translation (NAT)**

In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

**network hierarchy**

A type of container that is a hierarchical collection of network objects.

**network layer**

In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

**network object**

A component of a network hierarchy.

## O

---

**offense**

A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

**offsite source**

A device that is away from the primary site that forwards normalized data to an event collector.

**offsite target**

A device that is away from the primary site that receives event or data flow from an event collector.

**Open Source Vulnerability Database (OSVDB)**

Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

**open systems interconnection (OSI)**

The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

**OSI**

See [open systems interconnection](#).

**OSVDB**

See [Open Source Vulnerability Database](#).

## P

---

**parsing order**

A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

**payload data**

Application data contained in an IP flow, excluding header and administrative information.

**primary HA host**

The main computer that is connected to the HA cluster.

**protocol**

A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

## Q

---

**QID Map**

A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

## R

---

**R2L**

See [Remote To Local](#).

**R2R**

See [Remote To Remote](#).



**recon**

See [reconnaissance](#).

**reconnaissance (recon)**

A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

**reference map**

A data record of direct mapping of a key to a value, for example, a user name to a global ID.

**reference map of maps**

A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

**reference map of sets**

A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

**reference set**

A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

**reference table**

A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

**refresh timer**

An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

**relevance**

A measure of relative impact of an event, category, or offense on the network.

**Remote To Local (R2L)**

The external traffic from a remote network to a local network.

**Remote To Remote (R2R)**

The external traffic from a remote network to another remote network.

**report**

In query management, the formatted data that results from running a query and applying a form to it.

**report interval**

A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

**routing rule**

A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

**rule**

A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

## S

---

**scanner**

An automated security program that searches for software vulnerabilities within web applications.

**secondary HA host**

The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

**severity**

A measure of the relative threat that a source poses on a destination.

**Simple Network Management Protocol (SNMP)**

A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

**SNMP**

See [Simple Network Management Protocol](#).

**SOAP**

A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

**standby system**

A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

**subnet**

See [subnetwork](#).

**subnet mask**

For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

**subnetwork (subnet)**

A network that is divided into smaller independent subgroups, which still are interconnected.

**sub-search**

A function that allows a search query to be performed within a set of completed search results.

**superflow**

A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

**system view**

A visual representation of both primary and managed hosts that compose a system.

## T

---

**TCP**

See [Transmission Control Protocol](#).

**Transmission Control Protocol (TCP)**

A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also [Internet Protocol](#).

**truststore file**

A key database file that contains the public keys for a trusted entity.

## V

---

**violation**

An act that bypasses or contravenes corporate policy.

**vulnerability**

A security exposure in an operating system, system software, or application software component.

## W

---

**whois server**

A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

---

# Index

## A

- about [11](#)
- access category
  - description [168](#)
- Admin tab [7](#)
- aggregated data views
  - deleting [48](#)
  - disabling [48](#)
  - enabling [48](#)
  - managing [48](#)
- application category
  - description [193](#)
- audit category
  - description [219](#)
- authentication category
  - description [159](#)

## C

- changes
  - deploying [23](#)
- configuration [79](#)
- content
  - importing [140](#)
- content management tool
  - searching for custom content [59](#), [63](#), [64](#), [67](#)
- CRE category
  - custom rule event, *See* CRE
  - description [186](#)
- create [12](#)

## D

- data
  - obfuscation
    - decrypting [151](#)
- data obfuscation
  - creating a profile [150](#)
  - creating expressions [150](#)
  - overview [147](#)
- deleting a security profile [14](#)
- deploying changes [23](#)
- domains
  - creating [107](#), [108](#)
  - default domain [109](#)
  - domain-aware searches [109](#)
  - overlapping IP addresses [103](#)
  - rules and offenses [111](#)
  - segmenting your network [103](#)
  - tagging events and flows [104](#)
  - user-defined domains [109](#)
  - using security profiles [109](#)
- DoS category
  - description [156](#)
- duplicating a security profile [13](#)

## E

- edit [13](#)
- email, custom notifications [37](#), [40](#)
- encryption [19](#)
- event categories
  - description [153](#)
- event category correlation
  - access category [168](#)
  - application category [193](#)
  - audit category [219](#)
  - authentication category [159](#)
  - CRE category [186](#)
  - DoS category [156](#)
  - exploit category
    - description [170](#)
  - high-level categories [153](#)
  - malware category [172](#)
  - policy category [183](#)
  - potential exploit category [186](#)
  - recon category [154](#)
  - SIM Audit events category [192](#)
  - suspicious category [173](#)
  - system category [178](#)
  - unknown category [185](#)
  - User Defined category [189](#)
  - VIS host discovery category [193](#)
- Event Collector
  - about [15](#)
  - configuring [22](#)
- Event Processor
  - about [15](#)
- event retention
  - configuring [34](#)
  - deleting [36](#)
  - enabling and disabling [36](#)
  - managing [35](#)
  - sequencing [35](#)
- event view
  - building [15](#)
- events
  - domain creation [107](#), [108](#)
  - domain tagging [104](#)
  - storing and forwarding [137](#)
  - storing and forwarding events [137](#)
- exploit category [170](#)
- extensions
  - importing [140](#)
- external flow sources [87](#)

## F

- flow configuration [92](#)
- flow retention
  - configuring [34](#)
  - deleting [36](#)
  - enabling and disabling [36](#)

- flow retention (*continued*)
  - managing [35](#)
  - sequencing [35](#)
- flow source
  - about [87](#)
  - adding aliases [94](#)
  - adding flow source [92](#)
  - deleting aliases [94](#)
  - deleting flow source [93](#)
  - domain tagging [104](#)
  - editing aliases [94](#)
  - enabling or disabling [93](#)
  - external [87](#)
  - internal [87](#)
  - managing aliases [93](#)
  - virtual name [93](#)
- flow sources
  - domain creation [107](#), [108](#)
- flowlog file [92](#)
- forwarding destinations
  - in domain-aware environments [104](#)

## G

- glossary [249](#)

## H

- hiding data, *See* data obfuscation
- high-level categories
  - description [153](#)

## I

- importing content [140](#)
- internal flow sources [87](#)
- introduction [ix](#)
- IPv6
  - support and limitations [30](#)

## J

- J-Flow [91](#)

## M

- malware category
  - description [172](#)
- managed hosts
  - IPv6 support [30](#)
- managing [11](#)
- masking data, *See* data obfuscation

## N

- NAT
  - using with QRadar [18](#)
- NetFlow [88](#)
- network
  - domains [103](#)
- Network Address Translation. [18](#)
- network administrator [ix](#)

- network hierarchy
  - creating [25](#)
- network resources
  - suggested guidelines [99](#)
- new features
  - 7.4.1 [1](#)
  - Version 7.4.0 [3](#)

## O

- obfuscation
  - data
    - decrypting [151](#)
- offense close reason [43](#)
- offenses
  - domain-aware [111](#)
- overlapping IP addresses
  - domain segmentation [103](#)
- overview [79](#)

## P

- Packeteer [92](#)
- policy category
  - description [183](#)
- potential exploit category
  - description [186](#)

## R

- recon category
  - description [154](#)
- reference data collection [80](#)
- reference data collections [69](#)
- reference sets
  - adding [71](#)
  - adding elements [73](#)
  - deleting elements [74](#)
  - exporting elements [74](#)
  - viewing [71](#)
  - viewing contents [72](#)
- remote network groups
  - description [97](#)
- remote networks and services
  - description [97](#)
- remote networks object
  - adding [99](#)
- remote service groups
  - description [98](#)
- remote services object
  - adding [100](#)
- remote services objects
  - configuring [100](#)
- resetting SIM [24](#)
- retention buckets [33](#)
- roles [11](#)
- rules
  - domain-aware [111](#)

## S

- searching
  - in domain-aware environments [109](#)

- security profile [12–14](#)
- security profiles
  - domain privileges [109](#)
- servers
  - discovering [101](#)
- sFlow [91](#)
- SIM
  - resetting [24](#)
- SIM Audit category [192](#)
- SNMP traps
  - configuration overview [145](#)
- suspicious category
  - description [173](#)
- system category
  - description [178](#)
- system health [15](#)
- system management [15](#)
- system time [17](#)

## T

- time server configuration [17](#)
- Tivoli Directory Integrator server [79](#)

## U

- unknown category
  - description [185](#)
- User Defined category
  - description [189](#)
- user information [80](#)
- user information sources [79](#)
- user interface [7](#)
- users [11](#)

## V

- VIS host discovery category
  - description [193](#)

## W

- what's new [1](#), [3](#)





