IBM Security QRadar Log Manager
Version 7.2.0

Users Guide

IBM

Note: Before using this information and the product that it supports, read the information in “Notices and trademarks” on page 201.

CONTENTS

ABOUT THIS GUIDE

1 ABOUT QRADAR LOG MANAGER

2 DASHBOARD MANAGEMENT

6 CUSTOM EVENT PROPERTIES

7 RULE MANAGEMENT

ABOUT THIS GUIDE

The *IBM Security QRadar Log Manager Users Guide* provides information on managing IBM Security QRadar Log Manager including the **Dashboard**, **Log Activity**, and **Reports** tabs.

Intended audience

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

Conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION:*Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING:*Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting customer support

For information on contacting customer support, see the ***Support and Download Technical Note***. (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 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.

1 ABOUT QRADAR LOG MANAGER

IBM Security QRadar Log Manager is a network security management platform that provides situational awareness and compliance support through security event correlation, analysis, and reporting.

Supported web browsers

You can access the Console from a standard web browser. When you access the system, a prompt is displayed asking for a user name and a password, which must be configured in advance by the QRadar Log Manager administrator.

Table 1-1 Supported web browsers

Web browser	Supported versions
Mozilla Firefox	• 10.0 ESR • 17.0 ESR Due to Mozilla's short release cycle, we cannot commit to testing on the latest versions of the Mozilla Firefox web browser. However, we are fully committed to investigating any issues that are reported.
Microsoft® Windows Internet Explorer	• 8.0 • 9.0
Google Chrome	• Latest version We are fully committed to investigating any issue that are reported.

Logging in to QRadar Log Manager

QRadar Log Manager is a web-based application. To log in to QRadar Log Manager, you must use the Mozilla Firefox or Microsoft Internet Explorer web browsers.

For more information on supported web browsers, see **Supported web browsers**.

About this task

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

If you are using the Microsoft Internet Explorer web browser, a website security certificate message is displayed when you access the QRadar Log Manager system. You must select the **Continue to this website** option to log in to QRadar Log Manager.

Procedure

Step 1 Open your web browser.

Step 2 Type the following address in the address bar:

https://<`IP Address`>

Where **<`IP Address`>** is the IP address of the QRadar Log Manager system.

Step 3 Type your user name and password.

Step 4 Click **Login To QRadar**.

Step 5 To log out of QRadar Log Manager, click **Log out** in the top right corner of the user interface.

Result

A default license key provides you access to the user interface for five weeks. A window is displayed, providing the date that the temporary license key expires. For more information about installing a license key, see the *IBM Security QRadar Log Manager Administration Guide*.

When navigating QRadar Log Manager, do not use the browser **Back** button. Use the navigation options available with QRadar Log Manager to navigate the user interface.

User interface tabs

QRadar Log Manager divides functionality in tabs. The Dashboard tab is displayed when you log in to QRadar Log Manager. You can easily navigate the tabs to locate the data or functionality you require.

Dashboard tab

The **Dashboard** tab is the default tab that is displayed when you log in to QRadar Log Manager. It provides a workspace environment that provides summary and detailed information on events occurring in your network.

For more information about using the **Dashboard** tab, see **Dashboard management**.

Log Activity tab

The **Log Activity** tab allows you to investigate event logs being sent to QRadar Log Manager in real-time, perform powerful searches, and view log activity using configurable time-series charts. The **Log Activity** tab allows you to perform in-depth investigations on event data.

For more information, see **Log activity investigation**.

Reports tab

The **Reports** tab allows you to create, distribute, and manage reports for any data within QRadar Log Manager. The Reports feature allows you to create customized reports for operational and executive use. To create a report, you can combine information (such as, security or network) into a single report. You can also use pre-installed report templates that are included with QRadar Log Manager.

The **Reports** tab also allows you to brand your reports with customized logos. This is beneficial for distributing reports to different audiences.

For more information about reports, see **Reports management**.

Admin tab

If you have administrative privileges, you can access the **Admin** tab. The **Admin** tab gives administrative users access to administrative functionality, including:

- **System Configuration** - Allows you to configure system and user management options.
- **Data Sources** - Allows you to configure log sources.
- **Deployment Editor** - Allows you to manage the individual components of your QRadar Log Manager deployment.

All configuration updates you make in the **Admin** tab are saved to a staging area. When all changes are complete, you can deploy the configuration updates to the managed host in your deployment.

For more information regarding the **Admin** tab, see the *IBM Security QRadar Log Manager Administration Guide*.

QRadar Vulnerability Manager

QRadar Vulnerability Manager is a QRadar component that you can purchase separately and enable using a license key. QRadar Vulnerability Manager is a network scanning platform that provides awareness of the vulnerabilities that exist within the applications, systems, or devices on your network. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and re-run scans to evaluate the new level of risk.

When QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the **Vulnerabilities** tab. From the **Assets** tab, you can run QRadar Vulnerability Manager scans on selected assets.

For more information, see the *IBM Security QRadar Vulnerability Manager Users Guide*.

Assets tab

The Assets tab is only displayed if QRadar Vulnerability Manager is installed on your system.

QRadar Log Manager automatically discovers assets (servers and hosts) operating on your network, based on vulnerability data, allowing QRadar Log Manager to build an asset profile. Asset profiles provide information about each known asset in your network, including identity information (if available) and what services are running on each asset. This profile data is used for correlation purposes to help reduce false positives. For example, if an attack tries to exploit a specific service running on a specific asset, QRadar Log Manager can determine if the asset is vulnerable to this attack by correlating the attack to the asset profile. Using the **Assets** tab, you can view the learned assets or search for specific assets to view their profiles.

For more information, see **Asset management**.

QRadar Log Manager common procedures

Various controls on the QRadar Log Manager user interface are common to most user interface tabs. This section provides information on these common procedures.

Viewing messages

The Messages menu, which is located on the top right corner of the user interface, provides access to a window in which you can read and manage your system notifications.

Before you begin

For system notifications to show on the Messages window, the Administrator must create a rule based on each notification message type and select the **Notify** check box in the Custom Rules Wizard. For more information about how to configure event notifications and create event rules, see the *IBM Security QRadar Log Manager Administration Guid*e.

About this task

The Messages menu indicates how many unread system notifications you have in your system. This indicator increments the number until you dismiss system notifications. For each system notification, the Messages window provides a summary and the date stamp for when the system notification was created. You can hover your mouse pointer over a notification to view more detail. Using the functions on the Messages window, you can manage the system notifications.

System notifications are also available on the **Dashboard** tab and on an optional pop-up window that can be displayed on the lower left corner of the user interface. Actions that you perform in the Messages window are propagated to the **Dashboard** tab and the pop-up window. For example, if you dismiss a system notification from the Messages window, the system notification is removed from all system notification displays. For more information on Dashboard system notifications, see **System Notifications item**.

The Messages window provides the following functions:

Table 1-2 Messages window functions

Function	Description
All	Click **All** to view all system notifications. This is the default option, therefore, you only need to click **All** if you have selected another option and want to display all system notifications again.
Health	Click **Health** to view only system notifications that have a severity level of Health.
Errors	Click **Errors** to view only system notifications that have a severity level of Error.
Warnings	Click **Warnings** to view only the system notifications that have a severity level of Warning.
Information	Click **Information** to view only the system notifications that have a severity level of Information.
Dismiss All	Click **Dismiss All** to dismiss all system notifications from your system. If you have filtered the list of system notifications using the **Health**, **Errors**, **Warnings**, or **Information** icons, the text on the **View All** icon changes to one of the following options: • Dismiss All Errors • Dismiss All Health • Dismiss All Warnings • Dismiss All Info
View All	Click **View All** to view the system notification events in the **Log Activity** tab. If you have filtered the list of system notifications using the **Health**, **Errors**, **Warnings**, or **Information** icons, the text on the **View All** icon changes to one of the following options: • View All Errors • View All Health • View All Warnings • View All Info
Dismiss	Click the **Dismiss** icon beside a system notification to dismiss the system notification from your system.

When you click a notification, the following system notification details are displayed in a pop-up window:

Table 1-3 System notification details

Parameter	Description
Flag	Displays a symbol to indicate severity level of the notification. Point your mouse over the symbol to view more detail about the severity level. • Information icon (i) • Error icon (X) • Warning icon (!) • Health icon
Host IP	Displays the host IP address of the host that originated this system notification.
Severity	Displays the severity level of the incident that created this system notification.
Low Level Category	Displays the low-level category associated with the incident that generated this system notification. For example: Service Disruption. For more information on categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Payload	Displays the payload content associated with the incident that generated this system notification.
Created	Displays the amount of time that has elapsed since the system notification was created.

Procedure

Step 1 Log in to QRadar Log Manager.

Step 2 On the top right corner of the user interface, click **Messages**.

Step 3 On the Messages window, view the system notification details.

Step 4 Optional. To refine the list of system notifications, click one of the following options:

- Errors
- Warnings
- Information

Step 5 Optional. To dismiss system notifications, choose of the following options:

- To dismiss all system notifications, click **Dismiss All**.
- To dismiss one system notification, click the **Dismiss** icon next to the system notification you want to dismiss.

Step 6 Optional. To view the system notification details, hover your mouse pointer over the system notification.

Sorting results

On the **Log Activity** and **Reports** tabs, you can sort tables by clicking on a column heading. An arrow at the top of the column indicates the direction of the sort.

Procedure

Step 1 Log in to QRadar Log Manager.

Step 2 Click the tab you want to view:

Step 3 Choose one of the following options:

- Click the column header once to sort the table in descending order
- Click the column header twice to sort the table in ascending order.

Refreshing and pausing the user interface

The **Dashboard** and **Log Activity** tabs allow you to manually refresh, pause, and play the data displayed on the tab.

About this task

The **Dashboard** tab automatically refresh every 60 seconds. The **Log Activity** tab automatically refresh every 60 seconds if you are viewing the tab in Last Interval (auto refresh) mode. The timer, located at the top right corner of the interface, indicates the amount of time until the tab is automatically refreshed.

When you view the **Log Activity** tab in Real Time (streaming) or Last Minute (auto refresh) mode, you can use the **Pause** icon to pause the current display.

You can also pause the current display in the **Dashboard** tab. Clicking anywhere inside a dashboard item automatically pauses the tab. The timer flashes red to indicate the current display is paused.

Procedure

Step 1 Log in to QRadar Log Manager.

Step 2 Click the tab you want to view.

Step 3 Choose one of the following options:

- To refresh the tab, click the **Refresh** icon located in the right corner of the tab.
- To pause the display on the tab, click the **Pause** icon.
- If the time is paused, click the **Play** icon to restart the timer.

Investigating IP addresses

The **Dashboard** and **Log Activity** tabs provide several methods to investigate an IP address from the user interface.

About this task

The right-click menu provides options for you to investigate an IP address. You can add custom right-click options to the menu. For more information on how to customize the right-click menu, see the *Customizing the Right-Click Menu Technical Note*.

Procedure

Step 1 Log in to QRadar Log Manager.

Step 2 Click the tab you want to view.

Step 3 Move your mouse pointer over an IP address to view the location of the IP address.

Step 4 Right-click the IP address or asset name and select one of the following options from the Information menu:

Option	Description
DNS Lookup	Searches for DNS entries based on the IP address.
WHOIS Lookup	Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net.
Port Scan	Performs a Network Mapper (NMAP) scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information on installing NMAP, see your vendor documentation.
Search Events	Select the **Search Events** option to search events associated with this IP address. For information, see **Searching events**.
Information > Run QVM Scan	Select the Run QVM Scan option to scan a QRadar Vulnerability Manager scan on this IP address. This option is only displayed when QRadar Vulnerability Manager has been purchased and licensed. For more information, see the *QRadar Vulnerability Manager Users Guide.*

System time

The right corner of the QRadar Log Manager user interface displays system time, which is the time on the Console. The Console time synchronizes all QRadar Log Manager systems within the QRadar Log Manager deployment, and is used to determine what time events were received from other devices for proper time synchronization correlation.

In a distributed deployment, the Console might be located in a different time zone from your desktop computer. When you apply time-based filters and searches on the **Log Activity** tab, you must use the Console System Time when specifying a time range.

Updating user details

You can update your user details through the main QRadar Log Manager user interface.

Procedure

Step 1 To access your user information, click **Preferences**.

Step 2 As required, update the following parameters:

Options	Description
Username	Displays your user name. This field is not editable
Password	Type a new password. The password must meet the following criteria: • Minimum of six characters • Maximum of 255 characters • Contain at least one special character • Contain one uppercase character
Password (Confirm)	Type the password again for confirmation.
Email Address	Type your email address. The email address must meet the following requirements: • Valid email address • Minimum of 10 characters • Maximum of 255 characters
Enable Popup Notifications	Select this check box if you want to enable popup system notifications to be displayed on your user interface.

Accessing Online Help

You can access the QRadar Log Manager Online Help through the main QRadar Log Manager user interface. To access the Online Help, click **Help > Help Contents**.

Resizing columns

Several QRadar Log Manager tabs, including the **Log Activity** and **Reports** tabs allow you to resize the columns of the display. Place the pointer of your mouse over the line that separates the columns and drag the edge of the column to the new location. You can also resize columns by double-clicking the line that separates the columns to automatically resize the column to the width of the largest field.

Note: Column resizing does not function in Internet Explorer 7.0 while the **Log Activity** tab are displaying records in streaming mode.

Configuring page size

In the **Log Activity** and **Reports** tab tables, QRadar Log Manager displays a maximum of 40 results by default. If you have administrative privileges, you can configure the maximum number of results using the **Admin** tab. For more information, see the *IBM Security QRadar Log Manager Administration Guide*.

2 DASHBOARD MANAGEMENT

The **Dashboard** tab is the default view when you log into IBM Security QRadar Log Manager. It provides a workspace environment on which you can display your views of network security, activity, or data that QRadar Log Manager collects.

Dashboard overview

Use the **Dashboard** tab to monitor your security event behavior.

You can customize your dashboard. The content displayed on the **Dashboard** tab is user-specific. Changes made within a QRadar Log Manager session affect only your system.

To customize your **Dashboard** tab, you can perform the following tasks:

- Add and remove dashboard items from your dashboards.
- Move and position items to meet your requirements. When you position items, each item automatically resizes in proportion to the dashboard.
- Add custom dashboard items based on any data.

  For example, you can add a dashboard item that provides a time series graph or a bar chart that represents top 10 network activity.

  To create custom items, you can create saved searches on the **Log Activity** tab and choose how you want the results represented in your dashboard. Each dashboard chart displays real-time up-to-the-minute data. Time series graphs on the dashboard refresh every 5 minutes.

Available dashboard items

QRadar Log Manager allows you to add dashboard items to your default or custom dashboards.

Log Activity items

The Log Activity dashboard items allow you to monitor and investigate events in real-time.

Note: Hidden or closed events are not included in the values that are displayed in the **Dashboard** tab.

The following table describes the Log Activity items:

Table 2-4 Log activity items

Dashboard item	Description
Event Searches	You can display a custom dashboard item based on saved search criteria from the **Log Activity** tab. Event search items are listed in the **Add Item > Network Activity > Event Searches** menu. The name of the event search item matches the name of the saved search criteria the item is based on. QRadar Log Manager includes default saved search criteria that is preconfigured to display event search items on your **Dashboard** tab menu. You can add more event search dashboard items to your **Dashboard** tab menu. For more information, see **Adding search-based dashboard items to the Add Items list**. On a **Log Activity** dashboard item, search results display real-time last minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about chart configuration, see **Configuring charts**. Time series charts are interactive. You can magnify and scan through a timeline to investigate log activity.
Events By Severity	The **Events By Severity** dashboard item displays the number of active events grouped by severity. This item allows you to see the number of events that are received by the level of severity that has been assigned. Severity indicates the amount of threat an event source poses in relation to how prepared the destination is for the attack. The range of severity is 0 (low) to 10 (high). The supported chart types are Table, Pie, and Bar.
Top Log Sources	The **Top Log Sources** dashboard item displays the top five log sources that sent events to QRadar Log Manager within the last 5 minutes. The number of events sent from the specified log source is indicated in the pie chart. This item allows you to view potential changes in behavior, for example, if a firewall log source that is typically not in the top 10 list now contributes to a large percentage of the overall message count, you should investigate this occurrence. The supported chart types are Table, Pie, and Bar.

Most Recent Reports items

The **Most Recent Reports** dashboard item displays the top recently generated reports. The display provides the report title, the time and date the report was generated, and the format of the report.

System Summary item

The **System Summary** dashboard item provides a high-level summary of activity within the past 24 hours. Within the summary item, you can view the following information:

- **Current Events Per Second** - Displays the event rate per second.
- **New Events (Past 24 Hours)** - Displays the total number of new events received within the last 24 hours.

Vulnerability Management items

Vulnerability Management dashboard items are only displayed when IBM Security QRadar Vulnerability Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Vulnerability Manager Users Guide*.

You can display a custom dashboard item based on saved search criteria from the **Vulnerabilities** tab. Search items are listed in the **Add Item > Vulnerability Management > Vulnerability Searches** menu. The name of the search item matches the name of the saved search criteria the item is based on.

QRadar SIEM includes default saved search criteria that is preconfigured to display search items on your **Dashboard** tab menu. You can add more search dashboard items to your **Dashboard** tab menu.

The supported chart types are table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about chart configuration, see **Configuring charts**.

System Notifications item

The **Systems Notification** dashboard item displays event notifications your system receives. For notifications to show in the **System Notification** dashboard item, the Administrator must create a rule based on each notification message type and select the **Notify** check box in the Custom Rules Wizard. For more information about how to configure event notifications and create event rules, see the *IBM Security QRadar Log Manager Administration Guid*e.

On the **System Notifications** dashboard item, you can view the following information:

- **Flag** - Displays a symbol to indicate severity level of the notification. Point your mouse over the symbol to view more detail about the severity level.
  - **Health** icon
  - **Information** icon (?)
  - **Error** icon (X)
  - **Warning** icon (!)
- **Created** - Displays the amount of time that has elapsed since the notification was created.

- **Description** - Displays information about the notification.
- **Dismiss icon (x)**- Allows you to dismiss a system notification.

You can point your mouse over a notification to view more details:

- **Host IP** - Displays the host IP address of the host that originated the notification.
- **Severity** - Displays the severity level of the incident that created this notification.
- **Low Level Category** - Displays the low-level category associated with the incident that generated this notification. For example: Service Disruption. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide*.
- **Payload** - Displays the payload content associated with the incident that generated this notification.
- **Created** - Displays the amount of time that has elapsed since the notification was created.

When you add the **System Notifications** dashboard item, system notifications can also display as pop-up notifications in the QRadar Log Manager user interface. These pop-up notifications are displayed in the lower right corner of the user interface, regardless of the selected tab.

Pop-up notifications are only available for users with administrative permissions and are enabled by default. To disable pop-up notifications, select **User Preferences** and clear the **Enable Pop-up Notifications** check box. For more information, see the *IBM Security QRadar Log Manager Administration Guide*.

In the System Notifications pop-up window, the number of notifications in the queue is highlighted. For example, if (1 to 12) is displayed in the header, the current notification is 1 of 12 notifications to be displayed.

The system notification pop-up window provides the following options:

- **Next icon (>)** - Displays the next notification message. For example, if the current notification message is 3 of 6, click the icon to view 4 of 6.
- **Close icon (X)** - Closes this notification pop-up window.
- **(details)** - Displays additional information about this system notification.

Dashboard management tasks

You can customize your the **Dashboard** tab to display and organize the dashboards items that meet your network security requirements.

Adding dashboard items

You can add multiple dashboard items to your Dashboard tab.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the toolbar, click **Add Item**.

Step 3 Select the item you want to add. See **Available dashboard items**.

Investigating log or network activity from a dashboard item

You can investigate log activity from a dashboard item. Search-based dashboard items provide a link to the **Log Activity** tab. For more information on dashboard items, see **Available dashboard items**.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 Click the **View in Log Activity** link.

Result

When you open the **Log Activity** tab from the **Dashboard** tab, the data and two charts that match the parameters of your dashboard item are displayed. The chart types displayed on the **Log activity** tab depend on which chart is configured in the dashboard item:

- **Bar, Pie, and Table** - The **Log Activity** tab displays a bar chart, pie chart, and table of event details.
- **Time Series** - The **Log Activity** tab displays charts according to the following criteria:
  - If your time range is less than or equal to 1 hour, a time series chart, a bar chart, and a table of event details are displayed.
  - If your time range is more than 1 hour, a time series chart is displayed and you are prompted to click **Update Details**. This action starts the search that populates the event details and generates the bar chart. When the search completes, the bar chart and table of event details are displayed.

Configuring charts

You can configure **Log Activity** dashboard items to specify the chart type and how many data objects you want to view. Your custom chart configurations are retained, so that they are displayed as configured each time you access the **Dashboard** tab.

About this task

QRadar Log Manager accumulates data so that when you perform a time series saved search, there is a cache of event data available to display the data for the previous time period. Accumulated parameters are indicated by an asterisk (*) in the **Value to Graph** list box. If you select a value to graph that is not accumulated (no asterisk), time series data is not available.

For bar and pie charts that use accumulated data, the time range is displayed on the dashboard item. If the data is not yet accumulated for the full time range, the date and time for when accumulation started is also displayed.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 On the header of the dashboard item you want to configure, click the **Settings** icon.

Step 3 Configure the following parameters:

Option	Description
Value to Graph	From the list box, select the object type that you want to graph on the chart. Options include all normalized and custom event parameters included in your search parameters.
Chart Type	From the list box, select the chart type you want to view. Options include: • **Bar Chart** - Displays data in a bar chart. This option is only available for grouped events. • **Pie Chart** - Displays data in a pie chart. This option is only available for grouped events. • **Table** - Displays data in a table. This option is only available for grouped events. • **Time Series** - Displays an interactive line chart that represents the records matched by a specified time interval.
Display Top	From the list box, select the number of objects you want you view in the chart. Options include 5 and 10. The default is 10.
Capture Time Series Data	Select this check box to enable time series capture. When you select this check box, the chart feature begins to accumulate data for time series charts. By default, this option is disabled.
Time Range	From the list box, select the time range you want to view.

Removing items

You can remove items from a dashboard. When you remove an item from the dashboard, the item is not removed from QRadar Log Manager completely. You can add the item again at any time.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 On the dashboard item header, click the red [x] icon to remove the item from the dashboard.

Detaching an item

You can detach the item from your dashboard and display the item in a new window on your desktop system.

When you detach a dashboard item, the original dashboard item remains on the **Dashboard** tab, while a detached window with a duplicate dashboard item remains open and refreshes during scheduled intervals. If you close the QRadar Log Manager application, the detached window remains open for monitoring and continues to refresh until you manually close the window or shut down your computer system.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 On the dashboard item header, click the green icon to detach the dashboard item and open it in separate window.

Managing system notifications

You can specify the number of notifications that you want to display on your **System Notification** dashboard item and dismiss system notifications after you read them.

Before you begin

Ensure the **System Notification** dashboard item is added to your dashboard. For more information, see **Adding dashboard items**.

Procedure

Step 1 On the System Notification dashboard item header, click the **Settings** icon.

Step 2 From the **Display** list box, select the number of system notifications you want to view.

The options are **5**, **10** (default), **20**, **50**, and **All**.

To view all system notifications logged in the past 24 hours, click **All**. A window is displayed that includes all system notifications. For more information on events, see **Log activity investigation**.

Step 3 To dismiss a system notification, click the **Delete** icon.

Adding search-based dashboard items to the Add Items list

From the **Log Activity** and **Network Activity** tabs, you can add search-based dashboard items to your **Add Items** menu.

Before you begin

To add an event search dashboard item to the **Add Item** menu on the **Dashboard** tab, you must access the **Log Activity** or **Network Activity** tab to create search criteria that specifies that the search results can be displayed on the **Dashboard** tab. The search criteria must also specify that the results are grouped on a parameter.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, choose one of the following options:

- To create a new search, select **New Search**.
- To edit a saved search, select **Edit Search**.

Step 3 Configure or edit your search parameters, as required. For more information on event searches, see **Searching events**.

Ensure you configure the following parameters:

- On the Edit Search pane, select the **Include in my Dashboard** option.
- On the Column Definition pane, select a column and click the **Add Column** icon to move the column to the **Group By** list.

Step 4 Click **Filter**.

The search results are displayed.

Step 5 Click **Save Criteria**. See **Saving event search criteria**.

Step 6 Click **OK**.

Step 7 Verify that your saved search criteria successfully added the event search dashboard item to the **Add Items** list

a Click the **Dashboard** tab.

b To verify an event search item, select **Add Item > Log Activity > Event Searches**.

The dashboard item should be displayed on the list using the same name as your saved search criteria.

3 LOG ACTIVITY INVESTIGATION

Using the **Log Activity** tab, you can monitor and investigate log activity (events) in real-time or perform advanced searches.

Log Activity tab overview

An event is a record from a log source, such as a firewall or router device, that describes an action on a network or host.

You must have permission to view the **Log Activity** tab. For more information on permissions and assigning roles, see the *IBM Security QRadar Log Manager Administration Guide*.

Log Activity tab toolbar

Using the toolbar, you can access the following options:

Table 3-1 Log Activity tab toolbar options

Option	Description
Search	Click **Search** to perform advanced searches on events. Options include: • **New Search** - Select this option to create a new event search. • **Edit Search** - Select this option to select and edit an event search. • **Manage Search Results** - Select this option to view and manage search results. For more information about the search feature, see **Data searches**.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the **Quick Searches** list box only when you have saved search criteria that specifies the **Include in my Quick Searches** option.
Add Filter	Click **Add Filter** to add a filter to the current search results.
Save Criteria	Click **Save Criteria** to save the current search criteria.
Save Results	Click **Save Results** to save the current search results. This option is only displayed after a search is complete. This option is disabled in streaming mode.
Cancel	Click **Cancel** to cancel a search in progress. This option is disabled in streaming mode.

Table 3-1 Log Activity tab toolbar options (continued)

Option	Description
Rules	The Rules option is only visible if you have permission to view rules. Click **Rules** to configure custom event rules.
Actions	Click **Actions** to perform the following actions: • **Show All** - Select this option to remove all filters on search criteria and display all unfiltered events. • **Print** - Select this option to print the events displayed on the page. • **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See **Exporting events**. • **Export to XML > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See **Exporting events**. • **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See **Exporting events**. • **Export to CSV > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See **Exporting events**. • **Delete** - Select this option to delete a search result. See **Managing event search results**. • **Notify** - Select this option to specify that you want a notification emailed to you on completion of the selected searches. This option is only enabled for searches in progress. ***Note:*** *The* ***Print****,* ***Export to XML****, and* ***Export to CSV*** *options are disabled in streaming mode and when viewing partial search results.*
Quick Filter	Type your search criteria in the **Quick Filter** field and click the **Quick Filter** icon or press Enter on the keyboard. All events that match your search criteria are displayed in the events list. A text search is run on the event payload to determine which match your specified criteria. ***Note:*** *When you click the* ***Quick Filter*** *field, a tooltip is displayed, providing information on the appropriate syntax to use for search criteria. For more syntax information, see* ***Quick Filter syntax****.*

Quick Filter syntax

The Quick Filter feature enables you to search event payloads using a text search string. The Quick Filter functionality is available in the following locations on the user interface:

- **Log Activity toolbar** - On the toolbar, a **Quick Filter** field enables you to type a text search string and click the **Quick Filter** icon to apply your quick filter to the currently displayed list of events.
- **Add Filter dialog box** - From the **Add Filter** dialog box, accessed by clicking the **Add Filter** icon on the **Log Activity** tab, you can select **Quick Filter** as your filter parameter and type a text search string. This enables you to apply your quick filter to the currently displayed list of events. For more information about the Add Filter dialog box, see **Quick Filter syntax**.
- **Event search pages** - From the event search pages, you can add a Quick Filter to your list of filters to be included in your search criteria. For more information about configuring search criteria, see **Searching events**.

When viewing events in real time (streaming) or last interval mode, you can only type simple words or phrases in the **Quick Filter** field. When viewing events using a time-range, use the following syntax guidelines for typing your text search criteria:

- Search terms can include any plain text that you expect to find in the payload. For example, **`Firewall`**
- Include multiple terms in double quotes to indicate that you want to search for the exact phrase. For example, **`“Firewall deny"`**
- Search terms can include single and multiple character wild cards. The search term cannot start with a wild card. For example, **`F?rewall`** or **`F??ew*`**
- Search terms are matched in sequence from the first character in the payload word or phrase. For example, the search term **`user`** matches user_1 and user_2, but does not match the following phrases: ruser, myuser, or anyuser.
- Group terms using logical expressions, such as AND, OR, and NOT. The syntax is case sensitive and the operators must be upper case to be recognized as logical expressions and not as search terms. For example: **`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`**

  When creating search criteria that includes the NOT logical expression, you must include at least one other logical expression type, otherwise, your filter will not return any results. For example: **`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`**
- The following characters must be preceded by a backslash to indicate that the character is part of your search term: + - && || ! () {} [] ^ " ~ * ? : \. For example: **`"%PIX\-5\-304001"`**

Right-click menu options

On the **Log Activity** tab, you can right-click an event to access additional event filter information.

The right-click menu options are:

Table 3-2 Right-click menu options

Option	Description
Filter on	Select this option to filter on the selected event, depending on the selected parameter in the event.
More options:	Select this option to investigate an IP address or a user name. For more information about investigating an IP address, see **Investigating IP addresses**. ***Note:*** *This option is not displayed in streaming mode.*

Status bar

When streaming events, the status bar displays the average number of results received per second. This is the number of results the Console successfully received from the Event Processors. If this number is greater than 40 results per second, only 40 results are displayed. The remainder is accumulated in the result buffer. To view additional status information, move your mouse pointer over the status bar.

When QRadar Log Manager is not streaming events, the status bar displays the number of search results currently displayed on the tab and the amount of time required to process the search results.

Log activity monitoring

By default, the **Log Activity** tab displays events in streaming mode, allowing you to view events in real-time. For more information about streaming mode, see **Viewing streaming events**. You can specify a different time range to filter events using the **View** list box.

If you previously configured saved search criteria as the default, the results of that search are automatically displayed when you access the **Log Activity** tab. For more information about saving search criteria, see **Saving event search criteria**.

Viewing streaming events

Streaming mode enables you to view event data entering your system. This mode provides you with a real-time view of your current event activity by displaying the last 50 events.

About this task

If you apply any filters on the **Log Activity** tab or in your search criteria before enabling streaming mode, the filters are maintained in streaming mode. However, streaming mode does not support searches that include grouped events. If you enable streaming mode on grouped events or grouped search criteria, the **Log Activity** tab displays the normalized events. See **Viewing normalized events**.

When you want to select an event to view details or perform an action, you must pause streaming before you double-click an event. When streaming is paused, the last 1,000 events are displayed.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **View** list box, select **Real Time (streaming)**.

For information on the toolbar options, see **Table 3-1**. For more information about the parameters displayed in streaming mode, see **Table 3-7**.

Step 3 Optional. Pause or play the streaming events. Choose one of the following options:

- To select an event record, click the **Pause** icon to pause streaming.
- To restart streaming mode, click the **Play** icon.

Viewing normalized events

QRadar Log Manager collects events in raw format, and then normalizes the events for display on the **Log Activity** tab.

About this task

Normalization involves parsing raw event data and preparing the data to display readable information on the tab. When QRadar Log Manager normalizes events, the system normalizes names as well. Therefore, the name that is displayed on the **Log Activity** tab might not match the name that is displayed in the event.

Note: If you have selected a time frame to display, a time series chart is displayed. For more information about using time series charts, see **Time series chart overview**.

The **Log Activity** tab displays the following parameters when you view normalized events:

Table 3-3 Log Activity tab - Default (Normalized) parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filters applied to the search results. To clear these filter values, click **Clear Filter.** ***Note:*** *This parameter is only displayed after you apply a filter.*
View	From this list box, you can select the time range you want to filter for.

Table 3-3 Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to* ***Current Statistics*** *to display or hide the statistics* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.*
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Chart management**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that sent the event to QRadar Log Manager. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are detected within a short period of time.
Time	Specifies the date and time when QRadar Log Manager received the event.
Low Level Category	Specifies the low-level category associated with this event. For more information about event categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Source IP	Specifies the source IP address of the event.

Table 3-3 Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description
Source Port	Specifies the source port of the event.
Destination IP	Specifies the destination IP address of the event.
Destination Port	Specifies the destination port of the event.
Username	Specifies the user name associated with this event. User Names are often available in authentication related events. For all other types of events where the user name is not available, this field specifies N/A.
Magnitude	Specifies the magnitude of this event. Variables include credibility, relevance, and severity. Point your mouse over the magnitude bar to display values and the calculated magnitude. For more information about credibility, relevance, and severity, see the **Glossary**.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Display** list box, select **Default (Normalized)**.

Step 3 From the **View** list box, select the time frame you want to display.

Step 4 Click the **Pause** icon to pause streaming.

Step 5 Double-click the event you want to view in greater detail. See **Event details**.

Viewing raw events

You can view raw event data, which is the unparsed event data from the log source.

About this task

When you view raw event data, the **Log Activity** tab provides the following parameters for each event:

Table 3-4 Raw event parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filters applied to the search results. To clear these filter values, click **Clear Filter.** ***Note:*** *This parameter is only displayed after you apply a filter.*
View	From the list box, select the time range you want to filter for.

Table 3-4 Raw event parameters (continued)

Parameter	Description
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to **Current Statistics** to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.*
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Chart management**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To displayed charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Start Time	Specifies the time of the first event, as reported to QRadar Log Manager by the log source.
Log Source	Specifies the log source that originated the event. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Payload	Specifies the original event payload information in UTF-8 format.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Display** list box, select **Raw Events**.

Step 3 From the **View** list box, select the time frame you want to display.

Step 4 Double-click the event you want to view in greater detail. See **Event details**.

Viewing grouped events

Using the **Log Activity** tab, you can view events grouped by various options. From the **Display** list box, you can select the parameter by which you want to group events.

About this task

The **Display** list box is not displayed in streaming mode because streaming mode does not support grouped events. If you entered streaming mode using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

Table 3-5 Grouped events options

Group option	Description
Low Level Category	Displays a summarized list of events grouped by the low-level category of the event. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Event Name	Displays a summarized list of events grouped by the normalized name of the event.
Destination IP	Displays a summarized list of events grouped by the destination IP address of the event.
Destination Port	Displays a summarized list of events grouped by the destination port address of the event.
Source IP	Displays a summarized list of events grouped by the source IP address of the event.
Custom Rule	Displays a summarized list of events grouped by the associated custom rule.
Username	Displays a summarized list of events grouped by the user name associated with the events.
Log Source	Displays a summarized list of events grouped by the log sources that sent the event to QRadar Log Manager.
High Level Category	Displays a summarized list of events grouped by the high-level category of the event. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Network	Displays a summarized list of events grouped by the network associated with the event.
Source Port	Displays a summarized list of events grouped by the source port address of the event.

After you select an option from the **Display** list box, the column layout of the data depends on the chosen group option. Each row in the events table represents an event group. The **Log Activity** tab provides the following information for each event group:

Table 3-6 Grouped event parameters

Parameter	Description
Grouping By	Specifies the parameter that the search is grouped on.
Current Filters	The top of the table displays the details of the filter applied to the search results. To clear these filter values, click **Clear Filter**.
View	From the list box, select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to **Current Statistics** to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.*

Table 3-6 Grouped event parameters (continued)

Parameter	Description
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the chart from your display. Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent. Using the legend feature, you can perform the following actions: • Move your mouse pointer over a legend item to view more information about the parameters it represents. • Right-click the legend item to further investigate the item. For more information about right-click menu options, see **About QRadar Log Manager**. • Click a legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item. • Click **Legend** if you want to remove the legend from your chart display. ***Note:*** *The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see* **Chart management**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Source IP (Unique Count)	Specifies the source IP address associated with this event. If there are multiple IP addresses associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination IP (Unique Count)	Specifies the destination IP address associated with this event. If there are multiple IP addresses associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination Port (Unique Count)	Specifies the destination ports associated with this event. If there are multiple ports associated with this event, this field specifies the term Multiple and the number of ports.
Event Name	Specifies the normalized name of the event.
Log Source (Unique Count)	Specifies the log sources that sent the event to QRadar Log Manager. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
High Level Category (Unique Count)	Specifies the high-level category of this event. If there are multiple categories associated with this event, this field specifies the term Multiple and the number of categories. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide.*

Table 3-6 Grouped event parameters (continued)

Parameter	Description
Low Level Category (Unique Count)	Specifies the low-level category of this event. If there are multiple categories associated with this event, this field specifies the term Multiple and the number of categories. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Protocol (Unique Count)	Specifies the protocol ID associated with this event. If there are multiple protocols associated with this event, this field specifies the term Multiple and the number of protocol IDs.
Username (Unique Count)	Specifies the user name associated with this event, if available. If there are multiple user names associated with this event, this field specifies the term Multiple and the number of user names.
Magnitude (Maximum)	Specifies the maximum calculated magnitude for grouped events. Variables used to calculate magnitude include credibility, relevance, and severity. For more information about credibility, relevance, and severity, see the **Glossary**.
Event Count (Sum)	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Count	Specifies the total number of normalized events in this event group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **View** list box, select the time frame you want to display.

Step 3 From the **Display** list box, choose which parameter you want to group events on. See **Table 3-5**.

The events groups are listed. For more information on the event group details. See **Table 3-6**.

Step 4 To view the List of Events page for a group, double-click the event group you want to investigate.

The List of Events page does not retain chart configurations you might have defined on the **Log Activity** tab. For more information about the List of Events page parameters, see **Table 3-3**.

Step 5 To view the details of an event, double-click the event you want to investigate. For more information on event details, see **Table 3-7**.

Event details

You can view a list of event in various modes, including streaming mode or in event groups. In whichever mode you choose to view events, you can locate and view the details of a single event. The event details page provides the following information:

Table 3-7 Event details

Parameter	Description
Event Information	
Event Name	Specifies the normalized name of the event.
Low Level Category	Specifies the low-level category of this event. For more information about categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Event Description	Specifies a description of the event, if available.
Magnitude	Specifies the magnitude of this event. For more information about magnitude, see the **Glossary**.
Relevance	Specifies the relevance of this event. For more information about relevance, see the **Glossary**.
Severity	Specifies the severity of this event. For more information about severity, see the **Glossary**.
Credibility	Specifies the credibility of this event. For more information about credibility, see the **Glossary**.
Username	Specifies the user name associated with this event, if available.
Start Time	Specifies the time of the event was received from the log source.
Storage Time	Specifies the time that the event was stored in the QRadar Log Manager database.
Log Source Time	Specifies the system time as reported by the log source in the event payload.
Source and Destination Information	
Source IP	Specifies the source IP address of the event.
Destination IP	Specifies the destination IP address of the event.
Source Asset Name	Specifies the user-defined asset name of the event source.
Destination Asset Name	Specifies the user-defined asset name of the event destination.
Source Port	Specifies the source port of this event.
Destination Port	Specifies the destination port of this event.
Pre NAT Source IP	For a firewall or another device capable of Network Address Translation (NAT), this parameter specifies the source IP address before the NAT values were applied. NAT translates an IP address in one network to a different IP address in another network.
Pre NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address before the NAT values were applied.

Table 3-7 Event details (continued)

Parameter	Description
Pre NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port before the NAT values were applied.
Pre NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port before the NAT values were applied.
Post NAT Source IP	For a firewall or another device capable of NAT, this parameter specifies the source IP address after the NAT values were applied.
Post NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address after the NAT values were applied.
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
IPv6 Source	Specifies the source IPv6 address of the event.
IPv6 Destination	Specifies the destination IPv6 address of the event.
Source MAC	Specifies the source MAC address of the event.
Destination MAC	Specifies the destination MAC address of the event.
Payload Information	
Payload	Specifies the payload content from the event. This field offers three tabs to view the payload: • Universal Transformation Format (UTF) - Click **UTF**. • Hexadecimal - Click **HEX**. • Base64 - Click **Base64**.
Additional Information	
Protocol	Specifies the protocol associated with this event.
QID	Specifies the QID for this event. Each event has a unique QID. For more information about mapping a QID, see **Modifying event mapping**.
Log Source	Specifies the log source that sent the event to QRadar Log Manager. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Custom Rules	Specifies custom rules that match this event. For more information about rules, see the *IBM Security QRadar Log Manager Administration Guide.*

Table 3-7 Event details (continued)

Parameter	Description
Custom Rules Partially Matched	Specifies custom rules that partially match this event. For more information about rules, see the *IBM Security QRadar Log Manager Administration Guide.*
Annotations	Specifies the annotation for this event. Annotations are text descriptions that rules can automatically add to events as part of the rule response. For more information about rules, see the *IBM Security QRadar Log Manager Administration Guide*.
Identity Information - QRadar Log Manager collects identity information, if available, from log source messages. Identity information provides additional details about assets on your network. Log sources only generate identity information if the log message sent to QRadar Log Manager contains an IP address and least one of the following items: user name or MAC address. Not all log sources generate identity information.	
Identity Username	Specifies the user name of the asset associated with this event.
Identity IP	Specifies the IP address of the asset associated with this event.
Identity Net Bios Name	Specifies the Network Base Input/Output System (Net Bios) name of the asset associated with this event.
Identity Extended Field	Specifies additional information about the asset associated with this event. The content of this field is user-defined text and depends on the devices on your network that are available to provide identity information. Examples include: physical location of devices, relevant policies, network switch, and port names.
Has Identity (Flag)	Specifies True if QRadar Log Manager has collected identify information for the asset associated with this event. For more information about which devices send identity information, see the *IBM Security QRadar DSM Configuration Guide*.
Identity Host Name	Specifies the host name of the asset associated with this event.
Identity MAC	Specifies the MAC address of the asset associated with this event.
Identity Group Name	Specifies the group name of the asset associated with this event.

Event details toolbar

The event details toolbar provides the following functions:

Table 3-8 Event details toolbar

Function	Description
Return to Events List	Click **Return to Event List** to return to the list of events.
Map Event	Click **Map Event** to edit the event mapping. For more information, see **Modifying event mapping**.
Extract Property	Click **Extract Property** to create a custom event property from the selected event. For more information, see **Custom event properties**.

Table 3-8 Event details toolbar (continued)

Function	Description
Previous	Click **Previous** to view the previous event in the event list.
Next	Click **Next** to view the next event in the event list.
PCAP Data	***Note:*** *This option is only displayed if your QRadar Log Manager Console is configured to integrate with the Juniper JunOS Platform DSM. For more information about managing PCAP data, see* **Managing PCAP data**. From the **PCAP Data** list box, select one of the following options: • **View PCAP Information** - Select this option to view the PCAP information. For more information, see **Viewing PCAP information**. • **Download PCAP File** - Select this option to download the PCAP file to your desktop system. For more information, see **Downloading the PCAP file to your desktop system**.
Print	Click **Print** to print the event details.

Modifying event mapping

You can manually map a normalized or raw event to a high-level and low-level category (or QID). This manual action allows QRadar Log Manager to map unknown log source events to known QRadar Log Manager events so that they can be categorized and processed appropriately.

About this task

For normalization purposes, QRadar Log Manager automatically maps events from log sources to high- and low-level categories. For more information about event categories, see the *IBM Security QRadar Log Manager Administration Guide*.

When QRadar Log Manager receives events from log sources that the system is unable to categorize, QRadar Log Manager categorizes these events as unknown. These events occur for several reasons, including:

- **User-defined Events** - Some log sources, such as Snort, allow you to create user-defined events.
- **New Events or Older Events** - Vendor log sources might update their software with maintenance releases to support new events that QRadar Log Manager might not support.

Note: The **Map Event** icon is disabled for events when the high-level category is SIM Audit or the log source type is Simple Object Access Protocol (SOAP).

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event you want to map.

Step 4 Click **Map Event**.

Step 5 If you know the QID that you want to map to this event, type the QID in the **Enter QID** field. Go to **Step 7**.

Step 6 If you do not know the QID you want to map to this event, you can search for a particular QID:

a Choose one of the following options:

- To search for a QID by category, select the high-level category from the **High-Level Category** list box.
- To search for a QID by category, select the low-level category from the **Low-Level Category** list box.
- To search for a QID by log source type, select a log source type from the **Log Source Type** list box.
- To search for a QID by name, type a name in the **QID/Name** field.

b Click **Search**.

A list of QIDs are displayed.

c Select the QID you want to associate this event with.

Step 7 Click **OK**.

Managing PCAP data

If your QRadar Log Manager Console is configured to integrate with the Juniper JunOS Platform DSM, QRadar Log Manager can receive, process, and store Packet Capture (PCAP) data from a Juniper SRX-Series Services Gateway log source.

For more information about the Juniper JunOS Platform DSM, see the *IBM Security QRadar DSM Configuration Guide*.

Displaying the PCAP data column

The PCAP Data column is not displayed on the **Log Activity** tab by default. When you create search criteria, you must select the **PCAP Data** column in the Column Definition pane.

Before you begin

Before you can display PCAP data on the **Log Activity** tab, the Juniper SRX-Series Services Gateway log source must be configured with the PCAP Syslog Combination protocol. For more information about configuring log source protocols, see the *IBM Security QRadar Log Sources Users Guide*.

About this task

When you perform a search that includes the **PCAP Data** column, an icon is displayed in the **PCAP Data** column of the search results if PCAP data is available for an event. Using the **PCAP** icon, you can view the PCAP data or download the PCAP file to your desktop system.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **New Search**.

Step 3 Optional. To search for events that have PCAP data, configure the following search criteria:

- **a** From the first list box, select **PCAP data**.
- **b** From the second list box, select **Equals**.
- **c** From the third list box, select **True**.
- **d** Click **Add Filter**.

Step 4 Configure your column definitions to include the **PCAP Data** column:

- **a** From the **Available Columns** list in the Column Definition pane, click **PCAP Data**.
- **b** Click the **Add Column** icon on the bottom set of icons to move the **PCAP Data** column to the **Columns** list.
- **c** Optional. Click the **Add Column** icon in the top set of icons to move the **PCAP Data** column to the **Group By** list.

Step 5 Click **Filter**.

Step 6 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 7 Double-click the event you want to investigate.

What to do next

For more information about viewing and downloading PCAP data, see the following sections:

- **Viewing PCAP information**
- **Downloading the PCAP file to your desktop system**

Viewing PCAP information

From the **PCAP Data** toolbar menu, you can view the PCAP information or download the PCAP file to your desktop system. You can view a readable version of the data in the PCAP file.

Before you begin

Before you can view a PCAP information, you must perform or select a search that displays the **PCAP Data** column. See **Displaying the PCAP data column**.

About this task

Before PCAP data can be displayed, QRadar Log Manager must retrieve the PCAP file for display on the user interface. If the download process takes an extended period of time, the Downloading PCAP Packet Information window is displayed. In most cases, the download process is quick and this window is not displayed.

After the file is retrieved, a pop-up window provides a readable version of the PCAP file. You can read the information displayed on the window, or download the information to your desktop system

Procedure

Step 1 For the event you want to investigate, choose one of the following options:

- Select the event and click the **PCAP** icon.
- Right-click the **PCAP** icon for the event and select **More Options > View PCAP Information**.
- Double-click the event you want to investigate, and then select **PCAP Data > View PCAP Information** from the event details toolbar.

Step 2 If you want to download the information to your desktop system, choose one of the following options:

- Click **Download PCAP File** to download the original PCAP file to be used in an external application.
- Click **Download PCAP Text** to download the PCAP information in .TXT format.

Step 3 Choose one of the following options:

- If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
- If you want to save the list, select the **Save File** option.

Step 4 Click **OK**.

Downloading the PCAP file to your desktop system

You can download the PCAP file to your desktop system for storage or for use in other applications.

Before you begin

Before you can view a PCAP information, you must perform or select a search that displays the **PCAP Data** column. See Displaying the PCAP data column.

Procedure

Step 1 For the event you want to investigate, choose one of the following options:

- Select the event and click the **PCAP** icon.
- Right-click the **PCAP** icon for the event and select **More Options > Download PCAP File**.
- Double-click the event you want to investigate, and then select **PCAP Data > Download PCAP File** from the event details toolbar.

Step 2 Choose one of the following options:

- If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
- If you want to save the list, select the **Save File** option.

Step 3 Click **OK**.

Exporting events

You can export events in Extensible Markup Language (XML) or Comma Separated Values (CSV) format. The length of time required to export your data depends on the number of parameters specified.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 From the **Actions** list box, select one of the following options:

- **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to XML > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.
- **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to CSV > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.

Step 4 If you want to resume your activities while the export is in progress, click **Notify When Done**.

Result

When the export is complete, you receive notification that the export is complete. If you did not select the **Notify When Done** icon, the status window is displayed.

4 CHART MANAGEMENT

Using the charts on the **Log Activity** tab, you can view your data using various chart configuration options.

Charts overview

If you select a time frame or a grouping option to view your data on the **Log Activity** tab, charts display above the event list. Charts do not display while in streaming mode.

You can configure a chart to select what data you want to plot. You can configure charts independently of each other to display your search results from different perspectives.

Chart types include:

- **Bar Chart** - Displays data in a bar chart. This option is only available for grouped events.
- **Pie Chart** - Displays data in a pie chart. This option is only available for grouped events.
- **Table** - Displays data in a table. This option is only available for grouped events.
- **Time Series** - Displays an interactive line chart representing the records matched by a specified time interval. For information on configuring time series search criteria, see **Time series chart overview**.

After you configure a chart, your chart configurations are retained when you:

- Change your view using the **Display** list box.
- Apply a filter.
- Save your search criteria.

Your chart configurations are not retained when you:

- Start a new search.
- Access a quick search.

- View grouped results in a branch window.
- Save your search results.

Note: If you use the Mozilla Firefox web browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.

Time series chart overview

Time series charts are graphical representations of your log activity over time. Peaks and valleys displayed in the charts depict high and low volume activity. Time series charts are useful for short-term and long-term trending of data. Using time series charts, you can access, navigate, and investigate log activity from various views and perspectives.

Note: You must have the appropriate role permissions to manage and view time series charts. For more information about role permissions, see the *IBM Security QRadar Log Manager Administration Guide*.

To display time series charts, you must create and save a search that includes time series and grouping options. QRadar Log Manager supports up to 100 saved time series searches. QRadar Log Manager includes default time series saved searches, which you can access from the list of available searches on the event search page. You can easily identify saved time series searches on the **Quick Searches** menu, because the search name is appended with the time range specified in the search criteria.

If your search parameters match a previously saved search for column definition and grouping options, a time series chart might automatically display for your search results. If a time series chart does not automatically display for your unsaved search criteria, no previously saved search criteria exists to match your search parameters. If this occurs, you must enable time series data capture and save your search criteria.

You can magnify and scan a time line on a time series chart to investigate log activity. The following table provides functions you can use to view time series charts:

Table 4-1 Time series charts functions

Function	Description
View data in greater detail	Using the zoom feature, you can investigate smaller time segments of event traffic. • Move your mouse pointer over the chart, and then use your mouse wheel to magnify the chart (roll the mouse wheel up). • Highlight the area of the chart you want to magnify. When you release your mouse button, the chart displays a smaller time segment. Now you can click and drag the chart to scan the chart. When you magnify a time series chart, the chart refreshes to display a smaller time segment.
View a larger time span of data	Using the zoom feature, you can investigate larger time segments or return to the maximum time range. You can expand a time range using one of the following options: • Click **Zoom Reset** at the top left corner of the chart. • Move your mouse pointer over the chart, and then use your mouse wheel to expand the view (roll the mouse wheel down).
Scan the chart	When you have magnified a time series chart, you can click and drag the chart left or right to scan the time line.

Chart legends

Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent.

Using the legend feature, you can perform the following actions:

- Move your mouse pointer over a legend item or the legend color block to view more information about the parameters it represents.
- Right-click the legend item to further investigate the item. For more information about right-click menu options, see **About QRadar Log Manager**.
- Click a pie or bar chart legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item.
- Click **Legend**, or the arrow beside it, if you want to remove the legend from your chart display.

Configuring charts

You can use configuration options to change the chart type, the object type you want to chart, and the number of objects represented on the chart. For time series charts, you can also select a time range and enable time series data capture.

About this task

QRadar Log Manager can accumulate data so that when you perform a time series search, a cache of data is available to display data for the previous time period. After you enable time series data capture for a selected parameter, an asterisk (*) is displayed next to the parameter in the **Value to Graph** list box.

Before you begin

Charts are not displayed when you view events in Real Time (streaming) mode. To display charts, you must access the **Log Activity** tab, and choose one of the following options:

- Select options from the **View** and **Display** list boxes, and then click **Save Criteria** on the toolbar. See **Saving event search criteria**.
- On the toolbar, select a saved search from the **Quick Search** list box.
- Perform a grouped search, and then click **Save Criteria** on the toolbar. See **Searching events** and **Saving event search criteria**.

If you plan to configure a time series chart, ensure that the saved search criteria is grouped and specifies a time range.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 In the Charts pane, click the **Configure** icon.

Step 3 Configure values the following parameters:.

Parameters	**Description**
Value to Graph	From the list box, select the object type that you want to graph on the Y axis of the chart. Options include all normalized and custom event parameters included in your search parameters.
Display Top	From the list box, select the number of objects you want to view in the chart. The default is 10. Charting any more than 10 items might cause your chart data to be unreadable.
Chart Type	From the list box, select the chart type you want to view. If your bar, pie, or table chart is based on saved search criteria with a time range of more than 1 hour, you must click **Update Details** to update the chart and populate the event details.
Capture Time Series Data	Select this check box if you want to enable time series data capture. When you select this check box, the chart feature begins accumulating data for time series charts. By default, this option is disabled. This option is only available on Time Series charts.

Parameters	**Description**
Time Range	From the list box, select the time range you want to view. This option is only available on Time Series charts.

Step 4 If you selected the **Time Series** chart option and enabled the **Capture Time Series Data** option, click **Save Criteria** on the toolbar.

Step 5 To view the list of events if your time range is greater than 1 hour, click **Update Details**.

5 DATA SEARCHES

On the **Log Activity** tabs, you can search events using specific criteria. You can create a new search or load a previously saved set of search criteria. You can select, organize, and group the columns of data to be displayed in search results.

Searching events

On the **Log Activity** tab, you can search for events that match your search criteria.

About this task

When you perform a search, IBM Security QRadar Log Manager searches the entire database for events that match your criteria. This process might take an extended period of time depending on the size of your database.

The **Quick Filter** search parameter in the Search Parameters pane allows you to search for events that match your text string in the event payload. For more information about how to use the **Quick Filter** parameter, see **Quick Filter syntax**.

The following table describes the search options you can use to search event data:

Table 5-1 Event search options

Options	Description
Group	This list box allows you to select an event search group to view in the **Available Saved Searches** list.
Type Saved Search or Select from List	This field allows you to type the name of a saved search or a keyword to filter the **Available Saved Searches** list.
Available Saved Searches	This list displays all available searches, unless you apply a filter to the list using the **Group or Type Saved Search** or **Select from List** options. You can select a saved search on this list to display or edit.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Include in my Quick Searches	This check box allows you to include this search in your **Quick Search** menu, which is located on the **Log Activity** tab toolbar. For more information about the **Quick Search** menu, see **Log activity investigation**.

Table 5-1 Event search options

Options	Description
Include in my Dashboard	This check box allows you to include the data from your saved search on the **Dashboard** tab. For more information on the **Dashboard** tab, see **Dashboard management**. ***Note:*** *This parameter is only displayed if the search is grouped.*
Set as Default	This check box allows you to set this search as your default search when you access the **Log Activity** tab.
Share with Everyone	This check box allows you to share this search with all other users.
Real Time (streaming)	This option allows you to display event results in streaming mode. For more information on streaming mode, see **Viewing streaming events**. ***Note:*** *When Real Time (streaming) is enabled, you are unable to group your search results. If you select any grouping option in the Column Definition pane, an error message opens.*
Last Interval (auto refresh)	This option allows you the search results to display in auto-refresh mode. In auto-refresh mode, the **Log Activity** tab refresh at one minute intervals to display the most recent information.
Recent	This option allows you to select a predefined time range for your search. After you select this option, you must select a time range option from the list box.
Specific Interval	This option allows you to select a custom time range for your search. After you select this option, you must select the date and time range from the **Start Time** and **End Time** calendars.
Data Accumulation	This pane is only displayed when you load a saved search. Enabling unique counts on accumulated data that is shared with many other saved searches and reports may decrease system performance. When you load a saved search, this pane displays the following options: • If no data is accumulating for this saved search, the following information message is displayed: `Data is not being accumulated for this search`. • If data is accumulating for this saved search, the following options are displayed: **columns** - When you click or hover your mouse over this link, a list of the columns that are accumulating data opens. **Enable Unique Counts/Disable Unique Counts** - This link allows you to enable or disable the search results to display unique event counts instead of average counts over time. After you click the **Enable Unique Counts** link, a dialog box opens and indicates which saved searches and reports share the accumulated data.

Table 5-1 Event search options

Options	Description
Current Filters	This list displays the filters applied to this search. The options to add a filter are located above **Current Filters** list.
Save results when the search is complete	This check box allows you to save and name the search results.
Display	This list allows you to select a predefined column set to display in the search results.
Type Column or Select from List	You can use field to filter the columns that are listed in the **Available Columns** list. You can type the name of the column you want to locate or type a keyword to display a list of column names that include that keyword. For example, type **Device** to display a list of columns that include Device in the column name.
Available Columns	This list displays available columns. Columns that are currently in use for this saved search are highlighted and displayed in the **Columns** list.
Add and remove column icons (top set)	The top set of icons allows you to customize the **Group By** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** icon. • **Remove Column** - Select one or more columns from the **Group By** list and click the **Remove Column** icon.
Add and remove column icons (bottom set)	The bottom set of icon allows you to customize the **Columns** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** icon. • **Remove Column** - Select one or more columns from the **Columns** list and click the **Remove Column** icon.
Group By	This list specifies the columns on which the saved search groups the results. You can further customize the **Group By** list using the following options: • **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. • **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. The priority list specifies in which order the results are grouped. The search results are grouped by the first column in the **Group By** list and then grouped by the next column on the list.

Table 5-1 Event search options

Options	Description
Columns	Specifies columns chosen for the search. You can select more columns from the **Available Columns** list. You can further customize the **Columns** list by using the following options: • **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. • **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. If the column type is numeric or time-based and there is an entry in the **Group By** list, the column includes a list box to allow you to choose how you want to group the column. If the column type is group, the column includes a list box to allow you to choose how many levels you want to include for the group.
Order By	From the first list box, select the column by which you want to sort the search results. Then, from the second list box, select the order you want to display for the search results. Options include **Descending** and **Ascending**.

Procedure

Step 6 Click the **Log Activity** tab.

Step 7 From the **Search** list box, select **New Search**.

Step 8 Choose one of the following options:

- To load a previously saved search, go to **Step 9**.
- To create a new search, go to **Step 10**.

Step 9 Select a previously saved search:

a Choose one of the following options:

- From the **Available Saved Searches** list, select the saved search you want to load.
- In the **Type Saved Search or Select from List** field, type the name of the search you want to load.

b Click **Load**.

c In the Edit Search pane, select the options you want for this search. See **Table 5-1**.

Step 10 In the Time Range pane, select the options for the time range you want to capture for this search. See **Table 5-1**.

Step 11 Optional. In the Data Accumulation pane, enable unique counts:

a Click **Enable Unique Counts**.

b On the Warning window, read the warning message and click **Continue**. For more information on enabling unique counts, see **Table 5-1**.

Step 12 In the Search Parameters pane, define your search criteria:

a From the first list box, select a parameter you want to search for. For example, Device, Source Port, or Event Name.

b From the second list box, select the modifier you want to use for the search.

c In the entry field, type specific information related to your search parameter.

d Click **Add Filter**.

e Repeat steps a through d for each filter you want to add to the search criteria.

Step 13 Optional. To automatically save the search results when the search is complete, select the **Save results when search is complete** check box, and then type a name for the saved search.

Step 14 In the Column Definition pane, define the columns and column layout you want to use to view the results:

a From the **Display** list box, select the preconfigured column set to associate with this search.

b Click the arrow next to **Advanced View Definition** to display advanced search parameters.

c Customize the columns to display in the search results. See **Table 5-1**.

Step 15 Click **Filter**.

Result

When you generate a search that displays on the **Log Activity** tab before the search has collected all results, the partial results page is displayed. If the search is not complete, the **In Progress (<percent>% Complete)** status is displayed in the top right corner.

While viewing partial search results, the search engine works in the background to complete the search and refreshes the partial results to update your view.

When the search is complete, the **Completed** status is displayed in the top right corner.

Saving event search criteria

On the **Log Activity** tab, you can save configured search criteria so that you can re-use the criteria and use the saved search criteria in other QRadar Log Manager components, such as reports. Saved search criteria does not expire.

About this task

If you specify a time range for your search, QRadar Log Manager appends your search name with the specified time range. For example, a saved search named Exploits by Source with a time range of Last 5 minutes becomes Exploits by Source - Last 5 minutes.

If you change a column set in a previously saved search, and then save the search criteria using the same name, previous accumulations for time series charts are lost.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Perform a search. See **Searching events**.

The search results are displayed.

Step 3 Click **Save Criteria**.

Step 4 Enter values for the parameters:

Parameter	Description
Search Name	Type the unique name you want to assign to this search criteria.
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the **Other** group by default. For more information, see **Managing search groups**.
Manage Groups	Click **Manage Groups** to manage search groups. For more information, see **Managing search groups**.
Timespan options:	Choose one of the following options: • **Real Time (streaming)** - Select this option to filter your search results while in streaming mode. For more information about streaming mode, see **Viewing streaming events**. • **Last Interval (auto refresh)** - Select this option to filter your search results while in auto-refresh mode. The **Log Activity** tab refreshes at one minute intervals to display the most recent information. • **Recent** - Select this option and, from this list box, select the time range you want to filter for. • **Specific Interval** - Select this option and, from the calendar, select the date and time range you want to filter for.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is located on the **Log Activity** toolbar.
Include in my Dashboard	Select this check box to include the data from your saved search on the **Dashboard** tab. For more information about the **Dashboard** tab, see **Dashboard management**. ***Note:*** *This parameter is only displayed if the search is grouped.*
Set as Default	Select this check box to set this search as your default search when you access the **Log Activity** tab.
Share with Everyone	Select this check box to share these search requirements with all other QRadar Log Manager users.

Step 5 Click **OK**.

Deleting search criteria

If saved search criteria is no longer required, you can delete the search criteria.

About this task

When you delete a saved search, QRadar Log Manager objects that are associated with the saved search might no longer function. Reports and anomaly detection rules are QRadar Log Manager objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure they continue to function.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **New Search** or **Edit Search**.

Step 3 In the Saved Searches pane, select a saved search from the **Available Saved Searches** list box.

Step 4 Click **Delete**.

If the saved search criteria is not associated with other QRadar Log Manager objects, a confirmation window is displayed. See **Step 5**.

If the saved search criteria is associated with other QRadar Log Manager objects, the Delete Saved Search window is displayed. The window lists all QRadar Log Manager objects that are associated with the saved search you want to delete. Note the associated objects. See **Step 6**.

Step 5 Click **OK**.

Step 6 Choose one of the following options:

- Click **OK** to proceed. The saved search is now deleted.
- Click **Cancel** to close the Delete Saved Search window.

What to do next

If the saved search criteria was associated with other QRadar Log Manager objects, access the associated objects you noted and edit the objects to remove or replace the association with the deleted saved search.

Performing a sub-search

The sub-search feature allows you to perform searches within a set of previously completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again.

About this task

This feature is not available for grouped searches, searches in progress, or in streaming mode.

Before you begin

When defining a search that you want to use as a base for sub-searching, make sure that Real Time (streaming) option is disabled and the search is not grouped.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Perform a search. See **Searching events**.

Step 3 When your search is complete, add another filter:

- **a** Click **Add Filter**.
- **b** From the first list box, select a parameter you want to search for.
- **c** From the second list box, select the modifier you want to use for the search. The list of modifiers that are available depends on the attribute selected in the first list.
- **d** In the entry field, type specific information related to your search.
- **e** Click **Add Filter**.

Result

The Original Filter pane specifies the original filters applied to the base search. The Current Filter pane specifies the filters applied to the sub-search. You can clear sub-search filters without restarting the base search. Click the **Clear Filter** link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the base search is relaunched.

If you delete the base search criteria for saved sub-search criteria, you still have access to saved sub-search criteria. If you add a filter, the sub-search searches the entire database since the search function no longer bases the search on a previously searched data set

What to do next

Saving event search criteria

Managing event search results

You can initiate multiple event searches, and then navigate to other tabs to perform other tasks while your searches complete in the background. You can configure a search to send you an email notification when the search is complete. At any time while a search is in progress, you can return to the **Log Activity** tab to view partial or complete search results.

Saving search results

After you perform an event search, you can save the search results.

About this task

If you perform a search and do not explicitly save the search results, the search results are available on Manage Search Windows for 24 hours and then are automatically deleted.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Perform a search. See **Searching events**.

Step 3 Click **Save Results**.

Step 4 On the Save Search Result window, type a unique name for the search results.

Step 5 Click **OK**.

Viewing managed search results

Using the Manage Search Results page, you can view partial or complete search results.

About this task

Saved search results retain chart configurations from the associated search criteria, however, if the search result is based on search criteria that has been deleted, the default charts (bar and pie) are displayed.

The Manage Search Results page provides the following parameters:

Table 5-2 Manage Search Results page parameters

Parameter	Description
Flags	Indicates that an email notification is pending for when the search is complete.
User	Specifies the name of the user who started the search.
Name	Specifies the name of the search, if the search has been saved. For more information about saving a search, see **Saving search results**.
Started On	Specifies the date and time the search was started.
Ended On	Specifies the date and time the search ended.
Duration	Specifies the amount of time the search took to complete. If the search is currently in progress, the **Duration** parameter specifies how long the search has been processing to date. If the search was canceled, the **Duration** parameter specifies the period of time the search was processing before it was canceled.
Expires On	Specifies the date and time an unsaved search result will expire. The saved search retention figure is configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar Log Manager Administration Guide*.
Status	Specifies the status of the search. The statuses are: • **Queued** - Specifies that the search is queued to start. • **<percent>% Complete** - Specifies the progress of the search in terms of percentage complete. You can click the link to view partial results. • **Sorting** - Specifies that the search has finished collecting results and is currently preparing the results for viewing. • **Canceled** - Specifies that the search has been canceled. You can click the link to view the results that were collected before the cancellation. • **Completed** - Specifies that the search is complete. You can click the link to view the results. See **Log activity monitoring**.

Table 5-2 Manage Search Results page parameters (continued)

Parameter	Description
Size	Specifies the file size of the search result set.

The Manage Search Results window toolbar provides the following functions:

Table 5-3 Manage Search Results toolbar

Function	Description
New Search	Click **New Search** to create a new search. When you click this icon, the search page is displayed. See **Searching events**.
Save Results	Click **Save Results** to save the selected search results. See **Saving search results**.
Cancel	Click **Cancel** to cancel the selected search result that are in progress or are queued to start. See **Canceling a search**.
Delete	Click **Delete** to delete the selected search result. See **Deleting a search result**.
Notify	Click **Notify** to enable email notification when the selected search is complete.
View	From this list box, you can select which search results you want to list on the Search Results page. The options are: • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 View the list of search results. See **Table 5-2**.

What to do next

Canceling a search

Deleting a search result

Canceling a search

While a search is queued or in progress, you can cancel the search on the Manage Search Results page.

About this task

If the search is in progress when you cancel it, the results that were accumulated until the cancellation are maintained.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 Select the queued or in progress search result you want to cancel.

Step 4 Click **Cancel**.

Step 5 Click **Yes**.

Deleting a search result

If a search result is no longer required, you can delete the search result from the Manage Search Results page.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 Select the search result you want to delete.

Step 4 Click **Delete**.

Step 5 Click **Yes**.

Managing search groups

Using the Search Groups window, you can create and manage event search groups. These groups allow you to easily locate saved search criteria on the **Log Activity** and **Reports** tab.

Viewing search groups

QRadar Log Manager provides a default set of groups and subgroups, which you can view on the Event Search Group window.

About this task

All saved searches that are not assigned to a group are located in the **Other** group.

The Event Search Group window display the following parameters for each group:

Table 5-4 Search Group window parameters

Parameter	Description
Name	Specifies the name of the search group.
User	Specifies the name of the user that created the search group.
Description	Specifies the description of the search group.
Date Modified	Specifies the date the search group was modified.

The Event Search Group window toolbar provide the following functions:

Table 5-5 Search Group window toolbar functions

Function	Description
New Group	To create a new search group, you can click **New Group**. See **Creating a new search group**.
Edit	To edit an existing search group, you can click **Edit**. See **Editing a search group**.
Copy	To copy a saved search to another search group, you can click **Copy**. See **Copying a saved search to another groupe**.
Remove	To remove a search group or a saved search from a search group, select the item you want to remove, and then click **Remove**. See **Removing a group or a saved search from a group**.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 View the search groups. See **Table 5-4**.

What to do next

Creating a new search group

Editing a search group

Copying a saved search to another group

Removing a group or a saved search from a group

Creating a new search group

On the Event Search Group window, you can create a new search group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the folder for the group under which you want to create the new group.

Step 5 Click **New Group**.

Step 6 In the **Name** field, type a unique name for the new group.

Step 7 Optional. In the **Description** field, type a description.

Step 8 Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the group you want edit.

Step 5 Click **Edit**.

Step 6 Edit the parameters:

- Type a new name in the **Name** field.
- Type a new description in the **Description** field.

Step 7 Click **OK**.

Copying a saved search to another group

You can copy a saved search to another group. You can copy the saved search to more than one group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the saved search you want to copy.

Step 5 Click **Copy**.

Step 6 On the Item Groups window, select the check box for the group you want to copy the saved search to.

Step 7 Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the Remove icon to remove a search from a group or remove a search group.

About this task

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove the following groups from your system:

- Event Search Groups
- Other

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Choose one of the following options:

- Select the saved search you want to remove from the group.
- Select the group you want to remove.

Step 5 Click **Remove**.

Step 6 Click **OK**.

6 CUSTOM EVENT PROPERTIES

Custom event properties allow you to search, view, and report on information within logs that QRadar Log Manager does not typically normalize and display.

Custom property overview

You can create custom event properties from several locations on the **Log Activity** tab:

- **Event details** - You can select an event from the **Log Activity** tab to create a custom event property derived from its payload.
- **Search page** - You can create and edit a custom event or property from the Search page. When you create a new custom property from the Search page, the property is not derived from any particular event; therefore, the Custom Property Definition window does not prepopulate. You can copy and paste payload information from another source.

Required permissions

To create custom properties, you must have the **User Defined Event Properties** permission. If you have Administrative permissions, you can also create and modify custom properties from the **Admin** tab. Click **Admin > Data Sources > Custom Event Properties**. Check with your administrator to ensure you have the correct permissions. For more information regarding permissions, see the *IBM Security QRadar Log Manager Administration Guide*.

Custom property types

When you create a custom property, you can choose to create one of the following custom property type:

- **Regex** - Using regular expression (Regex) statements, you can extract unnormalized data from event payloads.

  For example, QRadar Log Manager reports on all users who make user permission changes on an Oracle server. QRadar Log Manager provides a list of users and the number of times they made a change to the permission of another account. However, QRadar Log Manager typically cannot display the actual user account or permission that was changed. You can create a custom property to extract this information from the logs, and then use the property in searches and reports.

  Use of this feature requires advanced knowledge of regular expressions (regex). Regex defines the field that you want to become the custom property.

After you enter a regex statement, you can validate it against the payload. When you define custom regex patterns, adhere to regex rules as defined by the Java™ programming language. For more information, you can refer to regex tutorials available on the web.

A custom property can be associated with multiple regular expressions. When an event is parsed, each regex pattern is tested on the event until a regex pattern matches the payload. The first regex pattern to match the event payload determines the data to be extracted.

- **Calculated** - Using calculation-based custom properties, you can perform calculations on existing numeric event properties to produce a calculated property. For example, you can create a property that displays a percentage by dividing one numeric property by another numeric property.

Custom property management

You can create, edit, copy, and delete custom properties.

Creating a regex-based custom property

You can create a regex-based customer property to match event payloads to a regular expression.

About this task

When you configure a regex-based custom property, the Custom Event Property windows provide the following parameters:

Table 6-1 Custom property definition window parameters (regex)

Parameter	Description
Test Field	Specifies the payload that was extracted from the unnormalized event.
Property Definition	
Existing Property	To select an existing property, select this option, and then select a previously saved property name from the list box.
New Property	To create a new property, select this option, and then type a unique name for this custom property. The new property name cannot be the name of a normalized property, such as *Username*, *Source IP*, or *Destination IP*.
Optimize parsing for rules, reports, and searches	To parse and store the property the first time QRadar Log Manager receives the event, select the check box. When you select the check box, the property does not require additional parsing for reporting, searching, or rule testing. If you clear this check box, the property is parsed each time a report, search, or rule test is performed. By default, this option is disabled.

Table 6-1 Custom property definition window parameters (regex) (continued)

Parameter	Description
Field Type	From the list box, select the field type. The field type determines how the custom property is displayed in QRadar Log Manager and which options are available for aggregation. The field type options are: • Alpha-Numeric • Numeric • IP • Port The default is Alpha-Numeric.
Description	Type a description of this custom property.
Property Expression Definition	
Log Source Type	From the list box, select the type of log source to which this custom event property applies. This parameter is only displayed on the Custom Event Property Definition window.
Log Source	From the list box, select the log source to which this custom event property applies. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources. This parameter is only displayed on the Custom Event Property Definition window.
Event Name	To specify an event name to which this custom property applies, select this option. Click **Browse** to access the Event Browser and select the QRadar Log Manager Identifier (QID) for the event name you want applied to this custom property. By default, this option is enabled.
Category	To specify a low-level category to which this custom property applies, select this option. To select a low-level category: **1** From the **High Level Category** list box, select the high-level category. The **Low Level Category** list updates to include only the low-level categories associated with the selected high-level category. **2** From the **Low Level Category** list box, select the low-level category to which this custom property applies.

Table 6-1 Custom property definition window parameters (regex) (continued)

Parameter	Description
RegEx	Type the regular expression you want to use for extracting the data from the payload. Regular expressions are case-sensitive. Sample regular expressions: • email: **`(.+@[^\.].*\.[a-z]{2,}$)`** • URL: **`(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)`** • Domain Name: **`(http[s]?://(.+?)["/?:])`** • Floating Point Number: **`([-+]?\d*\.?\d*$)`** • Integer: **`([-+]?\d*$)`** • IP Address: **`(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)`** For example: To match a log that resembles: **`SEVERITY=43`** Construct the following Regular Expression: **`SEVERITY=([-+]?\d*$)`** ***Note:*** *Capture groups must be enclosed in parenthesis.*
Capture Group	Type the capture group you want to use if the regex contains more than one capture group. Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses.
Test	Click **Test** to test the regular expression against the payload.
Enabled	Select this check box to enable this custom property. If you clear the check box, this custom property does not display in search filters or column lists and the property is not parsed from payloads. The default is Enabled.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event you want to base the custom property on.

Step 4 Click **Extract Property**.

Step 5 In the Property Type Selection pane, select the **Regex Based** option.

Step 6 Configure the custom property parameters. See Table 6-1.

Step 7 Click **Test** to test the regular expression against the payload.

Step 8 Click **Save**.

Results

The custom property is now displayed as an option in the list of available columns on the search page. To include a custom property in an events list, you must select the custom property from the list of available columns when creating a search.

Creating a calculation-based custom property

You can create a calculation-based customer property to match event payloads to a regular expression.

About this task

When you configure a calculation-based custom property, the Custom Event Property window provides the following parameters:

Table 6-2 Custom property definition window parameters (calculation)

Parameter	Description
Property Definition	
Property Name	Type a unique name for this custom property. The new property name cannot be the name of a normalized property, such as *Username*, *Source IP*, or *Destination IP*.
Description	Type a description of this custom property.
Property Calculation Definition	
Property 1	From the list box, select the first property you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the **Property 1** list box, select the **User Defined** option. The **Numeric Property** parameter is displayed. Type a specific numeric value.
Operator	From the list box, select the operator you want to apply to the selected properties in the calculation. Options include: • Add • Subtract • Multiply • Divide
Property 2	From the list box, select the second property you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the **Property 1** list box, select the **User Defined** option. The **Numeric Property** parameter is displayed. Type a specific numeric value.
Enabled	Select this check box to enable this custom property. If you clear the check box, this custom property does not display in event search filters or column lists and the event property is not parsed from payloads. The default is Enabled.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event you want to base the custom property on.

Step 4 Click **Extract Property**.

Step 5 In the Property Type Selection pane, select the **Calculation Based** option.

Step 6 Configure the custom property parameters. See **Table 6-2**.

Step 7 Click **Save**.

Results

The custom property is now displayed as an option in the list of available columns on the search page. To include a custom property in an events list, you must select the custom property from the list of available columns when creating a search.

Modifying a custom property

Using the Custom Event Properties window, you can modify a custom property.

About this task

The Custom Event Properties window provides the following information:

Table 6-3 Custom properties window columns

Column	Description
Property Name	Specifies a unique name for this custom property.
Type	Specifies the type for this custom property. Options include: • **Regex** - A regex-based custom property matches event payloads to a regular expression. See **Creating a regex-based custom property** • **Calculated** - A calculation-based custom property performs a calculation on event properties. See **Creating a calculation-based custom property**.
Property Description	Specifies a description for this custom property.
Log Source Type	Specifies the name of the log source type to which this custom property applies. This column is only displayed on the Custom Event Properties window.
Log Source	Specifies the log source to which this custom property applies. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources. This column is only displayed on the Custom Event Properties window.

Table 6-3 Custom properties window columns (continued)

Column	Description
Expression	Specifies the expression for this custom property. The expression depends on the custom property type: • For a regex-based custom property, this parameter specifies the regular expression you want to use for extracting the data from the payload. • For a calculation-based custom property, this parameter specifies the calculation you want to use to create the custom property value.
Username	Specifies the name of the user who created this custom property.
Enabled	Specifies whether this custom property is enabled. This field specifies either True or False.
Creation Date	Specifies the date this custom property was created.
Modification Date	Specifies the last time this custom property was modified.

The Custom Event Property toolbar provides the following functions:

Table 6-4 Custom property toolbar options

Option	Description
Add	Click **Add** to add a new custom property. See **Creating a regex-based custom property** or **Creating a calculation-based custom property**.
Edit	Click **Edit** to edit the selected custom property. See **Modifying a custom property**.
Copy	Click **Copy** to copy selected custom properties.
Delete	Click **Delete** to delete selected custom properties.
Enable/Disable	Click **Enable/Disable** to enable or disable the selected custom properties for parsing and viewing in the search filters or column lists.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to edit and click **Edit**.

Step 5 Edit the necessary parameters. See **Table 6-1**.

Step 6 Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.

Step 7 Click **Save**.

Copying a custom property

To create a new custom property that is based an existing custom property, you can copy the existing custom property, and then modify the parameters.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to copy and click **Copy**.

Step 5 Select the **New Property** option and type a new property name.

Step 6 Edit the necessary parameters. See **Table 6-1**.

Step 7 If you edited the regular expression, click **Test** to test the regular expression against the payload.

Step 8 Click **Save**.

Deleting a custom property

You can delete any custom property, provided the custom property is not associated with another custom property.

About this task

If you attempt to delete a custom property associated with another custom property, an error message is displayed to provide the name of the associated custom property.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to delete and click **Delete**.

Step 5 Click **Yes**.

7 RULE MANAGEMENT

From the **Log Activity** tab, you can view and maintain rules. This topic applies to users who have the **View Custom Rules** or **Maintain Custom Rules** user role permissions.

Rule permission considerations

You can view and manage rules for areas of the network that you can access if the you have the following user role permissions:

- View Custom Rules
- Maintain Custom Rules

Rules overview

Rules perform tests on events, and if all the conditions of a test are met, the rule generates a response. For a complete list of default rules, see **Default rules and building blocks**.

The tests in each rule can also reference other building blocks and rules. You are not required to create rules in any specific order because the system checks for dependencies each time a new rule is added, edited, or deleted. If a rule that is referenced by another rule is deleted or disabled, a warning is displayed and no action is taken.

Event rules

An event rule performs tests on events as they are processed in real-time by the Event Processor. You can create an event rule to detect a single event (within certain properties) or event sequences. For example, if you want to monitor your network for unsuccessful login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, you can create an event rule.

Rule conditions

Each rule might contain the following components:

- **Functions** - With functions, you can use building blocks and other rules to create a multi-event function. You can connect rules using functions that support Boolean operators, such as OR and AND. For example, if you want to connect event rules, you can use the **when an event matches any|all of the following rules** function. For a complete list of functions, see **Event rule tests**.
- **Building blocks** - A building block is a rule without a response and is used as a common variable in multiple rules or to build complex rules or logic that you want to use in other rules. You can save a group of tests as building blocks for use with other functions. Building blocks allow you to re-use specific rule tests in other rules. For example, you can save a building block that includes the IP addresses of all mail servers in your network and then use that building block to exclude those mail servers from another rule. The default building blocks are provided as guidelines, which should be reviewed and edited based on the needs of your network. For a complete list of building blocks, see **Default rules and building blocks**.
- **Tests** - You can run tests on the property of an event, such as source IP address, severity of event, or rate analysis. For a complete list of tests, see **Event rule tests**.

Rule responses

When rule conditions are met, a rule can generate one or more of the following responses:

- Send an email.
- Generate system notifications using the Dashboard feature.
- Add data to reference sets. For more information on reference sets, see the *IBM Security QRadar Log Manager Administration Guide*.
- Add data to reference data collections that can be used in rule tests. Before you can configure a rule to send data to a reference data collection, you must create the reference data collection using the Command Line Interface (CLI). For more information on how to create and use reference data collections, see *IBM Security QRadar Reference Data Collections* technical note.

  Using this option, you can add data to the following data collection types:

  - **Reference Map** - In a Reference Map, data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the **Username** parameter as a key and the user’s global ID as a value.
  - **Reference Map of Sets** - In a Reference Map of Sets, data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, you can create a Map of Sets that uses a custom event property for Patent ID as the key and the **Username** parameter as the value to populate a list of authorized users.
  - **Reference 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 single value. For example, to test for network bandwidth violations, you can create

a Map of Maps that uses the **Source IP** parameter as the first key, the **Application** parameter as the second key, and the **Total Bytes** parameter as the value.

- Generate a response to an external system, including the following server types:
    - **Local Syslog** - Syslog is a standard that allows you to store event information in a software-independent log file. Using the Rules wizard, you can configure rules to generate a syslog file.
    - **Forwarding Destinations** - A rule can forward raw log data received from log sources and normalized event data to one or more vendor systems, such as ticketing or alerting systems.
    - **Simple Network Management Protocol (SNMP)** - The SNMP protocol enables QRadar Log Manager to send event notifications to another host to be stored. Using the Rules wizard, you can configure rules to generate a response that sends SNMP traps to the configured host.
    - **Interface For Metadata Access Points (IF-MAP)** - The Interface For Metadata Access Points (IF-MAP) rule response enables the rule to publish event data derived from events data on an IF-MAP server.

Viewing rules

You can view the details of a rule, including the tests, building blocks, and responses.

Before you begin

Depending on your user role permissions, you can access the rules page from the **Log Activity** tab. For more information on user role permissions, see the *IBM Security QRadar Log Manager Administration Guide*.

About this task

The Rules page displays a list of rules with their associated parameters. For more information on the parameters displayed for each rule listed on the Rules page, see **Table 7-1**.

To locate the rule you want to open and view the details of, you can use the **Group** list box or **Search Rules** field on the toolbar. For more information on the Rules page toolbar, see **Table 7-2**.

Procedure

Step 1 Click the **Log Activity** tab, and then select **Rules** from the **Rules** list box on the toolbar.

Step 2 From the **Display** list box, select **Rules**.

Step 3 Double-click the rule you want to view.

Step 4 Review the rule details.

Results

If you have the **View Custom Rules** permission, but do not have the **Maintain Custom Rules** permission, the Rule Summary page is displayed and the rule cannot be edited.

If you have the **Maintain Custom Rules** permission, the Rule Test Stack Editor page is displayed. You can review and edit the rule details. See **Editing a rule**.

Creating a custom rule

QRadar Log Manager provides default rules, however, you can create new rules to meet the needs of your deployment.

About this task

To create a new rule, you must have the **Log Activity > Maintain Custom Rules** permission.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Actions** list box, select **New Event Rule**.

Step 4 Read the introductory text on the Rule Wizard. Click **Next**.

You are prompted to choose the source from which you want this rule to apply. The default is the rule type you selected in **Step 3**. You only need to choose a source on this page if you want to change your selection.

Step 5 Click **Next** to view the Rule Test Stack Editor page.

Step 6 In the **enter rule name here** field in the Rule pane, type a unique name you want to assign to this rule.

Step 7 From the list box, select whether you want to test the rule locally or globally:

- **Local** - The rule is tested on the local Event Processor and not shared with the system. The default is Local.
- **Global** - The rule is shared and tested by any Event Processor on the system. Global rules send events to the central Event Processor, which might decrease performance on the central Event Processor.

Step 8 Add one or more tests to a rule:

a Optional. To filter the options in the **Test Group** list box, type the text you want to filter for in the **Type to filter** field.

b From the **Test Group** list box, select the type of test you want to add to this rule.

c For each test you want to add to the rule, select the **+** sign beside the test.

d Optional. To identify a test as excluded test, click **and** at the beginning of the test in the Rule pane. The **and** is displayed as **and not**.

e Click the underlined configurable parameters to customize the variables of the test.

f From the dialog box, select values for the variable, and then click **Submit**.

Step 9 To export the configured rule as a building block to use with other rules:

a Click **Export as Building Block**.

b Type a unique name for this building block.

c Click **Save**.

Step 10 On the Groups pane, select the check boxes of the groups to which you want to assign this rule.

Step 11 In the **Notes** field, type a note that you want to include for this rule. Click **Next**.

Step 12 On the Rule Responses page, configure the responses you want this rule to generate. See Table 7-3.

Step 13 Click **Next**.

Step 14 Review the Rule Summary page to ensure the settings are correct. Make any changes if necessary, and then click **Finish**.

Rule management tasks

You can manage custom rules. You can enable and disable rules, as required. You can also edit, copy, or delete a rule.

Enabling/disabling rules

When tuning your system, you can enable or disable the appropriate rules to ensure that your system generates meaningful events for your environment.

About this task

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to enable or disable a rule.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box on the Rules page, select **Rules**.

Step 4 Select the rule you want to enable or disable.

Step 5 From the **Actions** list box, select **Enable/Disable**.

Editing a rule

You can edit a rule to change the rule name, rule type, tests, or responses.

About this task

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to edit a rule.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box on the Rules page, select **Rules**.

Step 4 Double-click the rule you want to edit.

Step 5 From the **Actions** list box, select **Open**.

Step 6 Optional. If you want to change the rule type, click **Back** and select a new rule type.

Step 7 On the Rule Test Stack Editor page, edit the parameters. See Table 7-1.

Step 8 Click **Next**.

Step 9 On the Rule Response page, edit the parameters. See Table 7-3.

Step 10 Click **Next**.

Step 11 Review the edited rule. Click **Finish**.

Copying a rule

To create a new rule, you can copy an existing rule, enter a new name for the rule, and then customize the parameters in the new rule as required.

About this task

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to copy a rule.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box, select **Rules**.

Step 4 Select the rule you want to duplicate.

Step 5 From the **Actions** list box, select **Duplicate**.

Step 6 In the **Enter name for the copied rule** field, type a name for the new rule. Click **OK**.

Deleting a rule

QRadar Log Manager allows you to delete a rule from your system.

About this task

You must have the **Log Activity > Maintain Custom Rules** role permission to be able to delete a rule.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box, select **Rules**.

Step 4 Select the rule you want to delete.

Step 5 From the **Actions** list box, select **Delete**.

Rule group management

If you are an administrator, you are able to create, edit, and delete groups of rules. Categorizing your rules or building blocks into groups allows you to efficiently view and track your rules. For example, you can view all rules related to compliance.

As you create new rules, you can assign the rule to an existing group. For information on assigning a group using the rule wizard, see **Creating a custom rule**.

Viewing a rule group

On the Rules page, you can filter the rules or building blocks to view only the rules or building blocks belonging to a specific group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box, select whether you want to view rules or building blocks.

Step 4 From the **Filter** list box, select the group category you want to view.

Result

The list of items assigned to that group displays.

Creating a group

The Rules page provides default rule groups, however, you can create a new group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the group under which you want to create a new group.

Step 5 Click **New Group**.

Step 6 Enter values for the following parameters:

- **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 Optional. To change the location of the new group, click the new group and drag the folder to the new location in your navigation tree.

Step 9 Close the Group window.

Assigning an item to a group

You can assign a selected rule or building block to a group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Select the rule or building block you want to assign to a group.

Step 4 From the **Actions** list box, select **Assign Groups**.

Step 5 Select the group you want to assign the rule or building block to.

Step 6 Click **Assign Groups**.

Step 7 Close the Choose Groups window.

Editing a group

You can edit a group to change the name or description.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the group you want to edit.

Step 5 Click **Edit**.

Step 6 Update values for the following parameters:

- **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 Optional. To change the location of the group, click the new group and drag the folder to the new location in your navigation tree.

Step 9 Close the Group window.

Copying an item to another group

Using the groups functionality, you can copy a rule or building block from one group to other groups.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the rule or building block you want to copy to another group.

Step 5 Click **Copy**.

Step 6 Select the check box for the group you want to copy the rule or building block to.

Step 7 Click **Copy**.

Step 8 Close the Group window.

Deleting an item from a group

You can delete an item from a group. When you delete an item from a group, the rule or building block is only deleted from group; it remains available on the Rules page.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Click **Groups**.

Step 4 Using the navigation tree, navigate to and select the item you want to delete.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Group window.

Deleting a group

You can delete a group. When you delete a group, the rules or building blocks of that group remain available on the Rules page.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 Click **Groups**.

Step 4 Using the navigation tree, navigate to and select the group you want to delete.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Group window.

Editing building blocks

QRadar Log Manager includes a set of default building blocks, which you can edit to match the needs of your deployment.

About this task

A building block is a re-usable rule test stack that you can include as a component in other rules.

For example, you can edit the BB:HostDefinition: Mail Servers building block to identify all mail servers in your deployment. Then, you can configure any rule to exclude your mail servers from the rule tests.

For more information about the default building blocks, see the *IBM Security QRadar Log Manager Administration Guide*.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 On the toolbar, click **Rules**.

Step 3 From the **Display** list box, select **Building Blocks**.

Step 4 Double-click the building block you want to edit.

Step 5 Update the building block, as necessary. Click **Next**.

Step 6 Continue through the wizard. For more information, see **Creating a custom rule**.

Step 7 Click **Finish**.

Rules page parameters

The list of deployed rules provides the following information for each rule:

Table 7-1 Rules page parameters

Parameter	Description
Rule Name	Displays the name of the rule.
Group	Displays the group to which this rule is assigned. For more information about groups, see **Rule group management**.
Rule Type	Displays the rule type.
Enabled	Indicates whether the rule is enabled or disabled. For more information about enabling and disabling rules, see **Enabling/disabling rules**.
Response	Displays the rule response, if any. Rule responses include: • Dispatch New Event • Email • Log • Notification • SNMP • Reference Set • Reference Data • IF-MAP Response For more information about rule responses, see **Rule responses**.
Origin	Displays whether this rule is a default rule (System) or a custom rule (User).
Creation Date	Specifies the date and time this rule was created.
Modification Date	Specifies the date and time this rule was modified.

Rules page toolbar

The Rules page toolbar provides the following functions:

Table 7-2 Rules page toolbar function

Function	Description
Display	From the list box, select whether you want to display rules or building blocks in the rules list.
Group	From the list box, select which rule group you want to be displayed in the rules list.
Groups	Click **Groups** to manage rule groups. For more information about grouping rules, see **Rule group management**.
Actions	Click **Actions** and select one of the following options: • **New Event Rule** - Select this option to create a new event rule. See **Creating a custom rule**. • **Enable/Disable** - Select this option to enable or disable selected rules. See **Enabling/disabling rules**. • **Duplicate** - Select this option to copy a selected rule. See **Copying a rule**. • **Edit** - Select this option to edit a selected rule. See **Editing a rule**. • **Delete** - Select this option to delete a selected rule. See **Deleting a rule**. • **Assign Groups** - Select this option to assign selected rules to rule groups. See **Assigning an item to a group**.
Revert Rule	Click **Revert Rule** to revert a modified system rule to the default value. When you click **Revert Rule**, a confirmation window is displayed. When you revert a rule, any previous modifications are permanently removed. ***Note:*** *To both revert the rule and maintain a modified version, duplicate the rule and use the* ***Revert Rule*** *option on the modified rule.*
Search Rules	Type your search criteria in the **Search Rules** field and click the **Search Rules** icon or press Enter on the keyboard. All rules that match your search criteria are displayed in the rules list. The following parameters are searched for a match with your search criteria: • Rule Name • Rule (description) • Notes • Response The Search Rule feature attempts to locate a direct text string match. If no match is found, the Search Rule feature then attempts a regular expression (regex) match.

Rule Response page parameters

Table 7-3 provides the Rule Response page parameters.

Table 7-3 Rule Response page parameters

Parameter	Description
Severity	Select this check box if you want this rule to set or adjust severity. When selected, you can use the list boxes to configure the appropriate severity level. For more information about severity, see the **Glossary**.
Credibility	Select this check box if you want this rule to set or adjust credibility. When selected, you can use the list boxes to configure the appropriate credibility level. For more information about credibility, see the **Glossary**.
Relevance	Select this check box if you want this rule to set or adjust relevance. When selected, you can use the list boxes to configure the appropriate relevance level. For more information about relevance, see the **Glossary**.
Annotate event	Select this check box if you want to add an annotation to this event and type the annotation you want to add to the event.
Drop the detected event	Select this check box to force an event, which is normally sent to the Magistrate component, to be sent to the Ariel database for reporting or searching.
Rule Response	
Dispatch New Event	Select this check box to dispatch a new event in addition to the original event, which will be processed like all other events in the system. The **Dispatch New Event** parameters are displayed when you select this check box. By default, the check box is clear.
Event Name	Type a unique name for the event you want to be displayed on the **Log Activity** tab.
Event Description	Type a description for the event. The description is displayed in the Annotations pane of the event details.
Severity	From the list box, select the severity for the event. The range is 0 (lowest) to 10 (highest) and the default is 0. The Severity is displayed in the Annotation pane of the event details. For more information about severity, see the **Glossary**.
Credibility	From the list box, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Credibility is displayed in the Annotation pane of the event details. For more information about credibility, see the **Glossary**.
Relevance	From the list box, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Relevance is displayed in the Annotations pane of the event details. For more information about relevance, see the **Glossary**.
High-Level Category	From the list box, select the high-level event category you want this rule to use when processing events. For more information about event categories, see the *IBM Security QRadar Log Manager Administration Guide*.

Table 7-3 Rule Response page parameters (continued)

Parameter	Description
Low-Level Category	From the list box, select the low-level event category you want this rule to use when processing events. For more information about event categories, see *IBM Security QRadar Log Manager Administration Guide*.
Email	Select this check box to display the email options. By default, the check box is clear.
Enter email addresses to notify	Type the email address to send notification if this rule generates. Separate multiple email addresses using a comma.
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar Log Manager Administration Guide*. ▶ Select this check box to enable this rule to send an SNMP notification (trap). The SNMP trap output includes system time, the trap OID, and the notification data, as defined by the IBM MIB. For more information about the IBM MIB, see the *IBM Security QRadar Log Manager Administration Guide*. For example, the SNMP notification might resemble: **`"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Event description"`**
Send to Local SysLog	Select this check box if you want to log the event locally. By default, this check box is clear. ***Note:*** *Only normalized events can be logged locally on a QRadar appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.* For example, the syslog output might resemble: **`Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description`**

Table 7-3 Rule Response page parameters (continued)

Parameter	Description
Send to Forwarding Destinations	This check box is only displayed for Event rules. Select this check box if you want to log the event on a forwarding destination. A forwarding destination is a vendor system, such as SIEM, ticketing, or alerting systems. When you select this check box, a list of forwarding destinations is displayed. Select the check box for the forwarding destination you want to send this event to. To add, edit, or delete a forwarding destination, click the **Manage Destinations** link. For more information about configuring forwarding destinations, see the *IBM Security QRadar Log Manager Administration Guide*.
Notify	Select this check box if you want events that generate as a result of this rule to be displayed in the System Notifications item on the Dashboard tab. For more information about the Dashboard tab, see **Dashboard management**. ***Note:*** *If you enable notifications, configure the **Response Limiter** parameter.*
Add to Reference Set	Select this check box if you want events generated as a result of this rule to add data to a reference set. To add data to a reference set: **1** Using the first list box, select the data you want to add. Options include all normalized or custom data. **2** Using the second list box, select the reference set to which you want to add the specified data. The **Add to Reference Set** rule response provides the following functions: • **Refresh** - Click **Refresh** to refresh the first list box to ensure that the list is current. • **Configure Reference Sets** - Click **Configure Reference Sets** to configure the reference set. This option is only available if you have administrative permissions. For more information on managing reference sets, see the *IBM Security QRadar Log Manager Administration Guide*.

Table 7-3 Rule Response page parameters (continued)

Parameter	Description
Add to Reference Data	Before you can use this rule response, you must create the reference data collection using the Command Line Interface (CLI). For more information on how to create and use reference data collections, see *IBM Security QRadar Reference Data Collections Technical Note*. Select this check box if you want events generated as a result of this rule to add to a reference data collection. After you select the check box, select one of the following options: • **Add to a Reference Map** - Select this option to send data to a collection of single key/multiple value pairs. You must select the key and value for the data record, and then select the reference map you want to add the data record to. • **Add to a Reference Map of Sets** - Select this option to send data to a collection of key/single value pairs. You must select the key and the value for the data record, and then select the reference map of sets you want to add the data record to. • **Add to a Reference Map of Maps** - Select this option to send data to a collection of multiple key/single value pairs. You must select a key for the first map, a key for the second map, and then the value for the data record. You must also select the reference map of maps you want to add the data record to.
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the event information on the IF-MAP server. For more information about configuring the IF-MAP parameters, see the *IBM Security QRadar Log Manager Administration Guide*.
Response Limiter	Select this check box and use the list boxes to configure the frequency in which you want this rule to respond.
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

Event rule tests

This section provides information on the event rule tests you can apply to the rules, including:

- **IP/Port tests**
- **Event property tests**
- **Common property tests**
- **Log source tests**
- **Function - Sequence tests**
- **Function - Counter tests**
- **Function - S**

- **Date/Time tests**
- **Function - Negative tests**

IP/Port tests The IP/Port tests include:

Table 7-4 Event Rule: IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valid when the source port of the event is one of the configured source ports.	when the source port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Destination Port	Valid when the destination port of the event is one of the configured destination ports.	when the destination port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Local Port	Valid when the local port of the event is one of the configured local ports.	when the local port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Remote Port	Valid when the remote port of the event is one of the configured remote ports.	when the remote port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Source IP Address	Valid when the source IP address of the event is one of the configured IP addresses.	when the source IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Destination IP Address	Valid when the destination IP address of the event is one of the configured IP addresses.	when the destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Local IP Address	Valid when the local IP address of the event is one of the configured IP addresses.	when the local IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Remote IP Address	Valid when the remote IP address of the event is one of the configured IP addresses.	when the remote IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
IP Address	Valid when the source or destination IP address of the event is one of the configured IP addresses.	when either the source or destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Source or Destination Port	Valid when either the source or destination port is one of the configured ports.	when the source or destination port is any of **these ports**	**these ports** - Specify the ports you want this test to consider.

Event property tests The event property test group includes:

Table 7-5 Event Rule: Event Property Tests

Test	Description	Default Test Name	Parameters
Local Network Object	Valid when the event occurs in the specified network.	when the **destination** network is **one of the following networks**	Configure the following parameters: • **source | destination** - Specify if you want this test to consider the source or destination IP address of the event. • **one of the following networks** - Specify the areas of the network you want this test to apply to.
IP Protocol	Valid when the IP protocol of the event is one of the configured protocols.	when the IP protocol is one of the following **protocols**	**protocols** - Specify the protocols you want to add to this test.
Event Payload Search	Each event contains a copy of the original unnormalized event. This test is valid when the entered search string is included anywhere in the event payload.	when the Event Payload contains **this string**	**this string** - Specify the text string you want to include for this test.
QID of Event	A QID is a unique identifier for events. This test is valid when the event identifier is a configured QID.	when the event QID is one of the following **QIDs**	**QIDs** - Use one of the following options to locate QIDs: • Select the Browse By Category option and from the list boxes, select the high and low-level category QIDs you want to locate. • Select the QID Search option and enter the QID or name you want to locate. Click **Search**.
Event Context	Event Context is the relationship between the source IP address and destination IP address of the event. For example, a local source IP address to a remote destination IP address. Valid if the event context is one of the following options: • Local to Local • Local to Remote • Remote to Local • Remote to Remote	when the event context is **this context**	**this context** - Specify the context you want this test to consider. The options are: • Local to Local • Local to Remote • Remote to Local • Remote to Remote

Table 7-5 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Event Category	Valid when the event category is the same as the configured category, for example, Denial of Service (DoS) attack.	when the event category for the event is one of the following **categories**	**categories** - Specify the event category you want this test to consider. For more information about event categories, see the *IBM Security QRadar Log Manager Administration Guide*.
Severity	Valid when the event severity is greater than, less than, or equal to the configured value.	when the event severity is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the severity is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.
Credibility	Valid when the event credibility is greater than, less than, or equal to the configured value.	when the event credibility is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the credibility is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.
Relevance	Valid when the event relevance is greater than, less than, or equal to the configured value.	when the event relevance is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the relevance is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.
Source Location	Valid when the source IP address of the event is either local or remote.	when the source is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic.
Destination Location	Valid when the destination IP address of the event is either local or remote.	when the destination is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic.
Rate Analysis	QRadar Log Manager monitors event rates of all source IP addresses/QIDs and destination IP addresses/QIDs and marks events that exhibit abnormal rate behavior. Valid when the event has been marked for rate analysis.	when the event has been marked with rate analysis	N/A

Table 7-5 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Regex	Valid when the configured MAC address, user name, host name, or operating system is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when the **username** matches the following **regex**	Configure the following parameters: • **MAC | source MAC | destination MAC | username | source username | destination username | event username | hostname | source hostname | dest hostname | OS | source OS | dest OS | event payload** - Specify the value you want to associate with this test. The default is **username**. • **regex** - Specify the regex string you want this test to consider.
IPv6	Valid when the source or destination IPv6 address is the configured IP address.	when the **source IP(v6)** is one of the following **IPv6 addresses**	Configure the following parameters: • **source IP(v6) | destination IP(v6)** - Specify whether you want this test to consider the source or destination IPv6 address. • **IP(v6) addresses** - Specify the IPv6 addresses you want this test to consider.
Reference Set	Valid when any or all configured event properties are contained in any or all configured reference sets.	when **any** of **these event properties** are contained in **any** of **these reference set(s)**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider.
Reference Map	Valid when any or all event properties in a configured key/value pair are contained within any or all configured reference maps.	when **any** of **these event properties** is the key and **any** of **these event properties** is the value in **any** of **these reference maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference maps** - Specify the reference maps you want this test to consider.

Table 7-5 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Reference Map of Sets	Valid when any or all event properties in a configured key/value pair are contained within any or all configured reference map of sets.	when **any** of **these event properties** is the key and **any** of **these event properties** is the value in **any** of **these reference map of sets**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference map of sets** - Specify the reference map of sets you want this test to consider.
Reference Map of Maps	Valid when any or all event properties in a configured primary and secondary key/value pair are contained within any or all configured reference map of maps.	when **any** of **these event properties** is the key of the first map and **any** of **these event properties** is the key of the second map and **any** of **these properties** is the value in any of **these reference map of maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference map of maps** - Specify the reference map of maps you want this test to consider.
Search Filter	Valid when the event matches the specified search filter.	when the event matches **this search filter**	**this search filter** - Specify the search filter you want this test to consider.

Common property tests

The common property test group includes:

Table 7-6 Event Rule: Common Property Tests

Test	Description	Default Test Name	Parameters
Custom Rule Engines	Valid when the event is processed by the specified Custom Rule Engines.	when the event is processed by one of **these** Custom Rule Engines	**these** - Specify the Custom Rule Engine you want this test to consider.

Table 7-6 Event Rule: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Regex	Valid when the configured property is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when any of **these properties** match the following **regex**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom event properties. • **regex** - Specify the regex string you want this test to consider.
Hexadecimal	Valid when the configured property is associated with particular hexadecimal values.	when any of **these properties** contain any of **these hexadecimal values**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom event properties. • **these hexadecimal values** - Specify the hexadecimal values you want this test to consider.

Log source tests The log source tests include:

Table 7-7 Event Rule: Log Source Tests

Test	Description	Default Test Name	Parameters
Source Log Sources	Valid when one of the configured log sources is the source of the event.	when the event(s) were detected by one or more of **these log sources**	**these log sources** - Specify the log sources that you want this test to detect.
Log Source Type	Valid when one of the configured log source types is the source of the event.	when the event(s) were detected by one or more of **these log source types**	**these log source types** - Specify the log sources that you want this test to detect.

Table 7-7 Event Rule: Log Source Tests (continued)

Test	Description	Default Test Name	Parameters
Inactive Log Sources	Valid when one of the configured log sources has not generated an event in the configured time.	when the event(s) have not been detected by one or more of **these log sources** for **this many** seconds	Configure the following parameters: **these log sources** - Specify the log sources that you want this test to detect. **this many** - Specify the number of time intervals you want this test to consider.
Log Source Groups	Valid when an event is detected by the configured log source groups.	when the event(s) were detected by one or more of **these log source groups**	**these log source groups** - Specify the groups you want this rule to consider.

Function - Sequence tests The function - sequence tests include:

Table 7-8 Event Rule: Functions - Sequence Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	You can use saved building blocks or other rules to populate this test. This function allows you to detect a specific sequence of selected rules involving a source and destination within a configured time period.	when all of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP,** over **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **username | source IP | source port | destination IP | destination port | QID | event ID | log source | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | username | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. You can use this function to detect a number of specified rules, in sequence, involving a source and destination within a configured time interval.	when at least **this number** of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP**, over **this many seconds**	Configure the following parameters: • **this number** - Specify the number of rules you want this function to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | username | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider.
Multi-Event Sequence Function Between Hosts	Allows you to detect a sequence of selected rules involving the same source and destination hosts within the configured time interval. You can also use saved building blocks and other rules to populate this test.	when this sequence of **rules**, involving the same source and destination hosts in **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a number of specific rules for a specific IP address or port followed by a number of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when at least **this many** of these **rules, in|in any** order, with the same **username** followed by at least **this many** of these **rules in| in any** order **to/from** the same **destination IP** from the previous sequence, within **this many minutes**	Configure the following parameters: • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify if you want this test to consider rules in a specific order. • **username | source IP | source port | destination IP | destination port** - Specify whether you want this test to consider the user name, source IP, source port, destination IP, or destination port. The default is **username**. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify if you want this test to consider rules in a specific order. • **to | from** - Specify the direction you want this test to consider. • **username | source IP | source port | destination IP | destination port** - Specify whether you want this test to consider the user name, source IP, source port, destination IP, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this rule to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect a configured number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties, and different event properties within the configured time interval after a series of specific rules.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Rule Function	Allows you to detect when specific rules occur a configured number of times in a configured time interval and after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties in a configured time interval and after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table 7-8 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

The function - counter tests include:

Table 7-9 Event Rule: Functions - Counters Group

Test	Description	Default Test Name	Parameters
Multi-Event Counter Function	Allows you to test the number of events from configured conditions, such as, source IP address. You can also use building blocks and other rules to populate this test.	when a(n) **source IP** matches **more than|exactly this many** of these **rules** across **more than|exactly this many destination IP,** over **this many minutes**	Configure the following parameters: • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of rules. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source above. • **this many** - Specify the number of IP addresses, ports, QIDs, events, log sources, or categories you want this test to consider. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time value you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table 7-9 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a series of rules for a specific IP address or port followed by a series of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when any of these **rules** with the same **source IP** more than **this many** times, across **more than| exactly this many destination IP** within **this many minutes**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **this many** - Specify the number of times the configured rules must match the test. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source option. • **this many** - Specify the number you want this test to consider, depending on the option you configured in the source IP parameter. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time interval you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table 7-9 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Username Function	Allows you to detect multiple updates to user names on a single host.	when the **username** changes more than **this many** times within **this many hours** on a single host.	Configure the following parameters: • **MAC | username | hostname** - Specify if you want this test to consider user name, MAC address, or host name. The default is **username**. • **this many** - Specify the number of changes you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **hours**.
Event Property Function	Allows you to detect a series of events with the same event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table 7-9 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a series of events with the same event properties and different event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address and different destination IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Rule Function	Allows you to detect a number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table 7-9 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Event Property Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

The function - simple tests include:

Table 7-10 Event Rule: Functions - Simple Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks and other rules to populate this test. The event has to match either all or any of the selected rules. If you want to create an OR statement for this rule test, specify the **any** parameter.	when an event matches **any|all** of the following **rules**	Configure the following parameters: • **any | all** - Specify either **any** or **all** of the configured rules that should apply to this test. • **rules** - Specify the rules you want this test to consider.

The date and time tests include:

Table 7-11 Event Rule: Date/Time Tests

Test	Description	Default Test Name	Parameters
Event Day	Valid when the event occurs on the configured day of the month.	when the event(s) occur **on** the **selected** day of the month	Configure the following parameters: • **on | after | before** - Specify if you want this test to consider on, after, or before the configured day. The default is **on**. • **selected** - Specify the day of the month you want this test to consider.
Event Week	Valid when the event occurs on the configured days of the week.	when the event(s) occur on any of **these days of the week**	**these days of the week** - Specify the days of the week you want this test to consider.
Event Time	Valid when the event occurs at, before, or after the configured time.	when the event(s) occur **after this time**	Configure the following parameters: • **after | before | at** - Specify if you want this test to consider after, before, or at the configured time. The default is **after**. • **this time** - Specify the time you want this test to consider.

The function - negative tests include:

Table 7-12 Event Rule: Functions - Negative Group

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when none of the specified rules in a configured time interval after a series of specific rules occur with the same event properties.	when none of **these rules** match in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.
Rule Function	Allows you to detect when none of the specified rules in a configured time interval after a series of specific rules occur.	when none of **these rules** match in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

8 ASSET MANAGEMENT

The **Asset** tab is only displayed on your QRadar Log Manager user interface if IBM Security QRadar Vulnerability Manager is installed on your system. QRadar Log Manager automatically discovers assets (servers and hosts) on your network, based on entity events and vulnerability data, to create asset profiles.

Asset profile overview

Asset profiles provide information about each known asset in your network, including what services are running on each asset. Asset profile information is used for correlation purposes to help reduce false positives. For example, if a source attempts to exploit a specific service running on an asset, QRadar Log Manager determines if the asset is vulnerable to this attack by correlating the attack to the asset profile.

Asset profiles are automatically discovered if you have vulnerability assessment (VA) scans configured. Asset profiles can also be automatically created from identity events. For more information about VA, see the *IBM Security QRadar Vulnerability Assessment Guide*.

Vulnerability overview

QRadar Log Manager identifies vulnerabilities using QRadar Vulnerability Manager and third-party scanners.

Third-party scanners identify and report discovered vulnerabilities to QRadar Log Manager using external references, such as the Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB), and Critical Watch. Examples of third-party scanners include QualysGuard and nCircle ip360. External references assign a unique reference identifier to each vulnerability. Examples of external data reference IDs include Common Vulnerability and Exposures (CVE) ID or Bugtraq ID. For more information on scanners and vulnerability assessment, see the *IBM Security QRadar Vulnerability Assessment Guide*.

QRadar Vulnerability Manager is an QRadar Log Manager component that you can purchase separately and enable using a license key. QRadar Vulnerability Manager is a network scanning platform that provides awareness of the vulnerabilities that exist within the applications, systems, or devices on your network. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and re-run scans to evaluate the new level of risk.

When QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the **Vulnerabilities** tab. From the **Assets** tab, you can run QRadar Vulnerability Manager scans on selected assets.

For more information, see the *IBM Security QRadar Vulnerability Manager Users Guide*.

Assets tab overview

The **Assets** tab provides you with a workspace from which you can manage your network assets and investigate an asset's vulnerabilities, ports, applications, history, and other associations.

Using the **Assets** tab, you can:

- View all the discovered assets.
- Manually add asset profiles.
- Search for specific assets.
- View information about discovered assets.
- Edit asset profiles for manually added or discovered assets.
- Tune false positive vulnerabilities.
- Import assets.
- Print or export asset profiles.
- Discover assets. For information about the Server Discovery option in the navigation pane, see the *IBM Security QRadar Log Manager Administration Guide*.
- Configure and manage third-party vulnerability scanning. For more information about the VA Scan option in the navigation pane, see the *IBM Security QRadar Vulnerability Assessment Guide.*
- Initiate QRadar Vulnerability Manager scans. For information, see the *IBM Security QRadar Vulnerability Management Guide*.

Asset tab list

The Asset Profiles page provides the following information on each asset:

Table 8-1 Asset Profile page parameters

Parameter	Description
ID	Displays the Asset ID number of the asset. QRadar Log Manager automatically generates the Asset ID number when you add an asset profile manually or when assets are discovered through events or vulnerability scans.
IP Address	Displays the last known IP address of the asset.

Table 8-1 Asset Profile page parameters (continued)

Parameter	Description
Asset Name	Displays the given name, NetBios name, or DSN name of the asset. If unknown, this field displays the last known IP address. ***Note:*** *These values are displayed in priority order. For example, if the asset does not have a given name, the aggregate NetBios name is displayed.* If the asset is automatically discovered, this field is automatically populated, however, you can edit the asset name if required.
Aggregate CVSS Score	Displays the one of the following Common Vulnerability Scoring System (CVSS) scores: • Coalesced aggregate environmental CVSS score • Aggregate temporal CVSS score • Aggregate CVSS base score ***Note:*** *These scores are displayed in priority order. For example, if the coalesced aggregate environmental CVSS score is not available, the aggregate temporal CVSS score is displayed.* A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. The CVSS score is calculated using the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see **Adding or editing an asset profile**. For more information on CVSS, see *http://www.first.org/cvss/*.
Vulnerabilities	Displays the number of unique vulnerabilities discovered on this asset. This value also includes the number of active and passive vulnerabilities.
Services	Displays the number of unique Layer 7 applications that run on this asset.

Assets tab toolbar

The Asset Profiles page toolbar provides the following functions:

Table 8-2 Asset Profiles page toolbar functions

Function	Description
Search	Click **Search** to perform advanced searches on assets. Options include: • **New Search** - Select this option to create a new asset search. • **Edit Search** - Select this option to edit an asset search. For more information about the search feature, see **Searching asset profiles**.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the **Quick Searches** list box only when you have saved search criteria that specifies the **Include in my Quick Searches** option.
Save Criteria	Click **Save Criteria** to save the current search criteria.
Add Filter	Click **Add Filter** to add a filter to the current search results.
Add Asset	Click **Add Asset** to add an asset profile. See **Adding or editing an asset profile**.
Edit Asset	Click **Edit Asset** to edit an asset profile. This option is enabled only if you have selected an asset profile from the results list. See **Adding or editing an asset profile**.
Actions	Click **Actions** to perform the following actions: • **Delete Asset** - Select this option to delete the selected asset profiles. See **Deleting assets**. • **Delete Listed** - Select this option to delete all asset profiles listed in the results list. See **Deleting assets**. • **Import Assets** - Select this option to import assets. See **Importing asset profiles**. • **Export to XML** - Select this option to export asset profiles in XML format. See **Exporting assets**. • **Export to CSV** - Select this option to export asset profiles in CSV format. See **Exporting assets**. • **Print** - Select this option to print the asset profiles displayed on the page. ***Note:*** *The **Actions** menu is available only if you have administrative privileges. For more information, see the IBM Security QRadar Log Manager Administration Guide.*
Clear Filter	After you apply a filter using the **Add Filter** option, you can click **Clear Filter** to remove the filter.

Right-click menu options

On the **Assets** tab, you can right-click an asset to access additional event filter information.

The right-click menu options are:

Table 8-3 Right-click menu options

Option	Description
Information	The Information menu provides the following options: • **DNS Lookup** - Searches for DNS entries based on the IP address. • **WHOIS Lookup** - Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net. • **Port Scan** - Performs a Network Mapper (NMAP) scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information about installing NMAP, see your vendor documentation. • **Asset Profile** - Displays asset profile information. This menu option is only available when QRadar Log Manager has acquired profile data either actively through a scan . For information, see the *IBM Security QRadar Log Manager Administration Guide*. • **Search Events** - Select the Search Events option to search events associated with this IP address. For information, see **Data searches**.
Run QVM Scan	Select this option to run a QRadar Vulnerability Manager scan on the selected asset. ***Note:*** *This option is displayed only after you install QRadar Vulnerability Manager. For more information, see the IBM Security QRadar Vulnerability Manager Users Guide.*

Viewing an asset profile

From the asset list on the **Assets** tab, you can select and view an asset profile. An asset profile provides information on each profile. Asset profile information is automatically discovered through Server Discovery or manually configured. You can edit automatically generated asset profile information.

About this task

The Asset Profile page provides the information about the asset organized into several panes. To view a pane, you can click the arrow (>) on the pane to view more detail or select the pane from the **Display** list box on the toolbar. Available panes include:

- **Asset Summary pane**
- **Network Interface Summary pane**
- **Vulnerability pane**
- **Services pane**
- **Windows Services pane**
- **Packages pane**
- **Windows Patches pane**
- **Properties pane**
- **Risk Policies pane**
- **Products pane**

The Asset Profile page toolbar provides the following functions:

Table 8-4 Asset Profile page toolbar functions

Options	Description
Return to Asset List	Click this option to return to the asset list.
Display	From the list box, you can select the pane you want to view on the Asset Profile pane. The Asset Summary and Network Interface Summary panes are always displayed. You can also display the following panes: • Asset Summary pane • Network Interface Summary pane • Vulnerability pane • Services pane • Windows Services pane • Packages pane • Windows Patches pane • Properties pane • Risk Policies pane • Products pane For more information about the parameters displayed in each pane, see **Assets profile page parameters**.
Edit Asset	Click this option to edit the Asset Profile. See **Adding or editing an asset profile**.

Table 8-4 Asset Profile page toolbar functions (continued)

Options	Description
History	Click **History** to view event history information for this asset. When you click the **History** icon, the Event Search window is displayed, pre-populated with the following event search criteria: • **Time Range** - Recent (Last 24 Hours) • **Search Parameters** - Specifies the following filters to be applied to the search results: - Identity is true - Identity IP is the IP address of the asset • **Column Definition** - Specifies the following columns to be displayed in the search results: - Event name - Log Source - Start Time - Identity User Name - Identity MAC - Identity Host Name - Identity Net Bios Name - Identity Group Name You can customize the search parameters, if required. Click **Search** to view the event history information. For more information about searching events, see **Data searches**.
Actions	From the **Actions** list, select **Vulnerability History**. This option is only displayed if QRadar Vulnerability Manager is installed in your deployment. For more information, see the *IBM Security QRadar Vulnerability Manager Users Guide*.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Double-click the asset you want to view.

Step 4 Use the options on the toolbar to display the various panes of asset profile information. See **Table 8-4**.

Step 5 To research the associated vulnerabilities, click each vulnerability in the Vulnerabilities pane. See **Table 8-10**.

Step 6 If required, edit the asset profile. See **Adding or editing an asset profile**.

Step 7 Click **Return to Assets List** to select and view another asset, if required.

Adding or editing an asset profile

QRadar Log Manager automatically discovers and adds asset profiles; therefore, adding an asset profile is typically not necessary. However, you might be required to manually add a profile.

When QRadar Log Manager discovers assets using the Server Discovery option, some asset profile details are automatically populated. You can manually add information to the asset profile and you can edit certain parameters.

About this task

You can only edit the parameters that were manually entered. Parameters that were system generated are displayed in italics and are not editable. You can delete system generated parameters, if required.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Choose one of the following options:

- To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.
- To edit an asset, double-click the asset you want to view and click **Edit Asset**.

Step 4 Configure the parameters in the MAC & IP Address pane. Configure one or more of the following options:

- Click the **New MAC Address** icon and type a MAC Address in the dialog box.
- Click the **New IP Address** icon and type an IP address in the dialog box.
- If **Unknown NIC** is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.
- Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.
- Select a MAC or IP address from the list and click the **Remove** icon.

Step 5 Configure the parameters in the Names & Description pane. Configure one or more of the following options:

Parameter	Description
DNS	Choose one of the following options: • Type a DNS name and click **Add**. • Select a DNS name from the list and click **Edit**. • Select a DNS name from the list and click **Remove**.

Parameter	Description
NetBIOS	Choose one of the following options: • Type a NetBIOS name and click **Add**. • Select a NetBIOS name from the list and click **Edit**. • Select a NetBIOS name from the list and click **Remove**.
Given Name	Type a name for this asset profile.
Location	Type a location for this asset profile.
Description	Type a description for the asset profile.
Wireless AP	Type the wireless Access Point (AP) for this asset profile.
Wireless SSID	Type the wireless Service Set Identifier (SSID) for this asset profile.
Switch ID	Type the switch ID for this asset profile.
Switch Port ID	Type the switch port ID for this asset profile.

Step 6 Configure the parameters in the Operating System pane:

a From the **Vendor** list box, select an operating system vendor.

b From the **Product** list box, select the operating system for the asset profile.

c From the **Version** list box, select the version for the selected operating system.

d Click the **Add** icon.

e From the **Override** list box, select one of the following options:

- **Until Next Scan** - Select this option to specify that the scanner provides operating system information and the information can be temporarily edited. If you edit the operating system parameters, the scanner restores the information at its next scan.
- **Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.

f Select an operating system from the list.

g Select an operating system and click the **Toggle Override** icon.

Step 7 Configure the parameters in the CVSS & Weight pane. Configure one or more of the following options:

Parameter	**Description**
Collateral Damage Potential	Configure this parameter to indicate the potential for loss of life or physical assets through damage or theft of this asset. You can also use this parameter to indicate potential for economic loss of productivity or revenue. Increased collateral damage potential increases the calculated value in the CVSS Score parameter. From the **Collateral Damage Potential** list box, select one of the following options: • None • Low • Low-medium • Medium-high • High • Not defined When you configure the **Collateral Damage Potential** parameter, the **Weight** parameter is automatically updated.
Confidentiality Requirement	Configure this parameter to indicate the impact on confidentiality of a successfully exploited vulnerability on this asset. Increased confidentiality impact increases the calculated value in the CVSS Score parameter. From the **Confidentiality Requirement** list box, select one of the following options: • Low • Medium • High • Not defined

Parameter	Description
Availability Requirement	Configure this parameter to indicate the impact to the asset's availability when a vulnerability is successfully exploited. Attacks that consume network bandwidth, processor cycles, or disk space impact the availability of an asset. Increased availability impact increases the calculated value in the CVSS Score parameter. From the **Availability Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Integrity Requirement	Configure this parameter to indicate the impact to the asset's integrity when a vulnerability is successfully exploited. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the calculated value in the CVSS Score parameter. From the **Integrity Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Weight	From the **Weight** list box, select a weight for this asset profile. The range is 0 to 10. When you configure the **Weight** parameter, the **Collateral Damage Potential** parameter is automatically updated.

Step 8 Configure the parameters in the Owner pane. Choose one or more of the following options:

Parameter	Description
Business Owner	Type the name of the business owner of the asset. An example of a business owner is a department manager. The maximum length is 255 characters.
Business Owner Contact	Type the contact information for the business owner. The maximum length is 255 characters.
Technical Owner	Type the technical owner of the asset. An example of a business owner is the IT manager or director. The maximum length is 255 characters.
Technical Owner Contact	Type the contact information for the technical owner. The maximum length is 255 characters.

Parameter	Description
Technical User	From the list box, select the QRadar Log Manager user name you want to associate with this asset profile. ***Note:*** *You can also use this parameter to enable automatic vulnerability remediation for IBM Security QRadar Vulnerability Manager. For more information about automatic remediation, see the IBM Security QRadar Vulnerability Manager User Guide.*

Step 9 Click **Save**.

Searching asset profiles

When you access the **Assets** tab, the Asset page is displayed populated with all discovered assets in your network. To refine this list, you can configure search parameters to display only the asset profiles you want to investigate.

About this task

From the Asset Search page, you can manage Asset Search Groups. For more information about Asset Search Groups, see **Asset search groups**.

The search feature allows you to search host profiles, assets, and identity information. Identity information provides additional details about log sources on your network, including DNS information, user logins, and MAC addresses.

Using the asset search feature, you can search for assets by external data references to determine if known vulnerabilities exist in your deployment.

For example:

You receive a notification that CVE ID: CVE-2010-000 is being actively exploited in the field. To verify if any hosts in your deployment are vulnerable to this exploit, you can select **Vulnerability External Reference** from the list of search parameters, select **CVE**, and then type the `2010-000` to view a list of all hosts that are vulnerable to that specific CVE ID.

Note: For more information about OSVDB, see *http://osvdb.org/*. For more information about NVDB, see *http://nvd.nist.gov/*.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 On the toolbar, click **Search > New Search**.

Step 4 Choose one of the following options:

- To load a previously saved search, go to **Step 5**.
- To create a new search, go to **Step 6**.

Step 5 Select a previously saved search:

a Choose one of the following options:

- Optional. From the **Group** list box, select the asset search group you want to display in the **Available Saved Searches** list.
- From the **Available Saved Searches** list, select the saved search you want to load.
- In the **Type Saved Search or Select from List** field, type the name of the search you want to load.

b Click **Load**.

Step 6 In the Search Parameters pane, define your search criteria:

a From the first list box, select the asset parameter you want to search for. For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.

b From the second list box, select the modifier you want to use for the search.

c In the entry field, type specific information related to your search parameter.

d Click **Add Filter**.

e Repeat these steps for each filter you want to add to the search criteria.

Step 7 Click **Search**.

What to do next

You can save your asset search criteria. See **Saving asset search criteria**.

Saving asset search criteria

On the **Asset** tab, you can save configured search criteria so that you can re-use the criteria. Saved search criteria does not expire.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Perform a search. See **Searching asset profiles**.

The search results are displayed.

Step 4 Click **Save Criteria**.

Step 5 Enter values for the parameters:

Parameter	Description
Enter the name of this search	Type the unique name you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. For more information, see **Asset search groups**. This option is only displayed if you have administrative permissions.

Parameter	Description
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the **Other** group by default. For more information, see **Asset search groups**.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is located on the **Assets** tab toolbar.
Set as Default	Select this check box to set this search as your default search when you access the **Assets** tab.
Share with Everyone	Select this check box to share these search requirements with all other QRadar Log Manager users.

Step 6 Click **OK**.

Asset search groups

Using the Asset Search Groups window, you can create and manage asset search groups. These groups allow you to easily locate saved search criteria on the **Assets** tabs.

Viewing search groups

Use the Asset Search Groups window to view a list groups and subgroups. From this window, you can view details about each group, including a description and the date the group was last modified.

About this task

All saved searches that are not assigned to a group are located in the **Other** group.

The Asset Search Groups window displays the following parameters for each group:

Table 8-5 Asset Search Groups window parameters

Parameter	Description
Name	Specifies the name of the search group.
User	Specifies the name of the user that created the search group.
Description	Specifies the description of the search group.
Date Modified	Specifies the date the search group was modified.

The Asset Search Groups window toolbars provide the following functions:

Table 8-6 Asset Search Groups window toolbar functions

Function	Description
New Group	To create a new search group, you can click **New Group**. See **Creating a new search group**.

Table 8-6 Asset Search Groups window toolbar functions (continued)

Function	Description
Edit	To edit an existing search group, you can click **Edit**. See **Editing a search group**.
Copy	To copy a saved search to another search group, you can click **Copy**. See **Copying a saved search to another group**.
Remove	To remove a search group or a saved search from a search group, select the item you want to remove, and then click **Remove**. See **Removing a group or a saved search from a group**.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select **Search > New Search**.

Step 4 Click **Manage Groups**.

Step 5 View the search groups. See **Table 8-5**.

What to do next

Creating a new search group

Editing a search group

Copying a saved search to another group

Removing a group or a saved search from a group

Creating a new search group

On the Asset Search Groups window, you can create a new search group.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select **Search > New Search**.

Step 4 Click **Manage Groups**.

Step 5 Select the folder for the group under which you want to create the new group.

Step 6 Click **New Group**.

Step 7 In the **Name** field, type a unique name for the new group.

Step 8 Optional. In the **Description** field, type a description.

Step 9 Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select **Search > New Search**.

Step 4 Click **Manage Groups**.

Step 5 Select the group you want to edit.

Step 6 Click **Edit**.

Step 7 Edit the parameters:

- Type a new name in the **Name** field.
- Type a new description in the **Description** field.

Step 8 Click **OK**.

Copying a saved search to another group

You can copy a saved search to another group. You can also copy the saved search to more than one group.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select **Search > New Search**.

Step 4 Click **Manage Groups**.

Step 5 Select the saved search you want to copy.

Step 6 Click **Copy**.

Step 7 On the Item Groups window, select the check box for the group you want to copy the saved search to.

Step 8 Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the Remove icon to remove a search from a group or remove a search group.

About this task

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove the following groups from your system:

- Asset Search Groups
- Other

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select **Search > New Search**.

Step 4 Click **Manage Groups**.

Step 5 Choose one of the following options:

- Select the saved search you want to remove from the group.
- Select the group you want to remove.

Step 6 Click **Remove**.

Step 7 Click **OK**.

Asset profile management tasks

Using the **Assets** tab, you can delete, import, and export asset profiles.

Deleting assets

You can delete specific assets or all listed asset profiles.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Choose one of the following options:

- Select the asset you want to delete, and then select **Delete Asset** from the **Actions** list box.
- From the **Actions** list box, select **Delete Listed**.

Step 4 Click **OK**.

Importing asset profiles

You can import asset profile information into QRadar Log Manager.

Before you begin

The imported file must be a CSV file in the following format:

```
ip,name,weight,description
```

Where:

- **IP** - Specifies any valid IP address in the dotted decimal format. For example: 192.168.5.34.
- **Name** - Specifies the name of this asset up to 255 characters in length. Commas are not valid in this field and invalidate the import process. For example: WebServer01 is correct.

- **Weight** - Specifies a number from 0 to 10, which indicates the importance of this asset on your network. A value of 0 denotes low importance and 10 is very high.
- **Description** - Specifies a textual description for this asset up to 255 characters in length. This value is optional.

For example, the following entries might be included in a CSV file:

```
192.168.5.34,WebServer01,5,Main Production Web Server
192.168.5.35,MailServ01,0,
```

The import process merges the imported asset profiles with the asset profile information you have currently stored in the system.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 From the **Actions** list box, select **Import Assets**.

Step 4 Click **Browse** to locate and select the CSV file you want to import.

Step 5 Click **Import Assets** to begin the import process.

Result

If an error occurs during the import process, no assets are imported.

Exporting assets

You can export listed asset profiles to an Extended Markup Language (XML) or Comma-Separated Value (CSV) file.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 From the **Actions** list box, select one of the following options:

- Export to XML
- Export to CSV

A status window provides the status of the export process.

Step 4 Optional. If you want to use other tabs and pages in QRadar Log Manager while the export is in progress, click the **Notify When Done** link.

When the export is complete, the File Download window is displayed.

Step 5 On the File Download window, choose one of the following options:

- **Open** - Select this option to open the export results in your choice of browser.
- **Save** - Select this option to save the results to your desktop.

Step 6 Click **OK**.

Research asset vulnerabilities

The Vulnerabilities pane on the Asset Profile page displays a list of discovered vulnerabilities for the asset. You can double-click the vulnerability to display more vulnerability details.

About this task

The Research Vulnerability Details window provides the following details:

Table 8-7 Research Vulnerabilities Details window details

Parameter	Description
Vulnerability ID	Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Published Date	Specifies the date on which the vulnerability details were published on the OSVDB.
Name	Specifies the name of the vulnerability.
Assets	Specifies the number of assets in your network that have this vulnerability. Click the link to view the list of assets.
Assets, including exceptions	Specifies the number of assets in your network that have vulnerability exceptions. Click the link to view the list of assets.
CVE	Specifies the CVE identifier for the vulnerability. CVE identifiers are provided by the NVDB. Click the link to obtain more information. When you click the link, the NVDB website is displayed in a new browser window.
xforce	Specifies the X-Force identifier for the vulnerability. Click the link to obtain more information. When you click the link, the IBM Internet Security Systems website is displayed in a new browser window.
OSVDB	Specifies the OSVDB identifier for the vulnerability. Click the link to obtain more information. When you click the link, the OSVDB website is displayed in a new browser window.

Table 8-7 Research Vulnerabilities Details window details (continued)

Parameter	**Description**
CVSS Score	Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. The CVSS score is calculated using the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see **Adding or editing an asset profile**. For more information on CVSS, see *http://www.first.org/cvss/*.
Impact	Displays the type of harm or damage that can be expected if this vulnerability is exploited.
CVSS Base Metrics	Displays the metrics used to calculate the CVSS base score, including: • Access Vector • Access complexity • Authentication • Confidentiality impact • Integrity impact • Availability impact
Description	Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.
Concern	Specifies the effects the vulnerability can have on your network.
Solution	Follow the instructions provided to resolve the vulnerability.
Virtual Patching	Displays virtual patch information associated with this vulnerability, if available. A virtual patch is a short-term mitigation solution for a recently discovered vulnerability. This information is derived from Intrusion Protection System (IPS) events. If you want to install the virtual patch, see your IPS vendor information.

Table 8-7 Research Vulnerabilities Details window details (continued)

Parameter	Description
Reference	Displays a list of external references, including: • **Reference Type** - Specifies the type of reference listed, such as an advisory URL or mail post list. • **URL** - Specifies the URL that you can click to view the reference. Click the link to obtain more information. When you click the link, the external resource is displayed in a new browser window.
Products	Displays a list of products that are associated with this vulnerability. • **Vendor** - Specifies the vendor of the product. • **Product** - Specifies the product name. • **Version** - Specifies the version number of the product.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Select an asset profile.

Step 4 In the Vulnerabilities pane, click the **ID** or **Vulnerability** parameter value for the vulnerability you want to investigate.

Step 5 Review the information on the Research Vulnerability Details page.

Assets profile page parameters

This reference includes tables that describe the parameters displayed in each pane of the Asset Profile tab.

Asset Summary pane

The Asset Summary pane on the Asset Profile page provides the following information:

Table 8-8 Asset Summary pane parameters

Parameter	Description
Asset ID	Displays the ID number that QRadar Log Manager assigned to the asset profile.
IP Address	Displays the last reported IP address of the asset.
MAC Address	Displays the last known MAC address of the asset.
Network	Displays the last reported network associated with the asset.
NetBIOS Name	Displays the NetBIOS name of the asset, if known. If the asset has more than one NetBIOS name, this field indicates the number of NetBIOS names. Move your mouse pointer over the value to view a list of associated NetBIOS names.

Table 8-8 Asset Summary pane parameters (continued)

Parameter	Description
DNS Name	Displays the IP address or DNS name of the asset, if known. If the asset has more than one DNS name, this field indicates the number of DNS names. Move your mouse pointer over the value to view a list of associated DNS names.
Given Name	Displays the name of the asset. By default, this field is empty. To provide a given name for the asset, edit the asset profile.
Group Name	Displays the last known user group of the asset, if known.
Last User	Displays the last known user of the asset. QRadar Log Manager derives user information from identity events. If more than one user is associated with this asset, you can click the link to display all users.
Operating System	Displays the operating system running on the asset. If the asset has more than one operating system, this field indicates the number of operating systems. Move your mouse pointer over the value to view a list of associated operating systems. ***Note:*** *You can edit this parameter directly if the* ***Override*** *parameter is specified as* ***Until the Next Scan*** *or* ***Forever****.*
Weight	Displays the level of importance associated with this asset. The range is 0 (Not Important) to 10 (Very Important). By default, this field is empty. To provide a weight for the asset, edit the asset profile.
Aggregate CVSS Score	Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. The CVSS score is calculated using the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see **Adding or editing an asset profile**. For more information on CVSS, see *http://www.first.org/cvss/*.
Business Owner	Displays the name of the business owner of the asset. An example of a business owner is a department manager.
Business Owner Contact Info	Displays the contact information for the business owner.

Table 8-8 Asset Summary pane parameters (continued)

Parameter	Description
CVSS Collateral Damage Potential	Displays the potential this asset has for collateral damage. This value is included in the formula to calculate the **CVSS Score** parameter. Options include: • None • Low • Low-medium • Medium-high • High • Not defined By default this field is not defined. To provide a location for the asset, edit the asset profile.
Technical Owner	Displays the technical owner of the asset. An example of a technical owner is an IT manager or director.
Technical Owner Contact Info	Displays the contact information of the technical owner.
CVSS Availability	Displays the impact to the asset’s availability when a vulnerability is successfully exploited. Options include: • Low • Medium • High • Not defined
Wireless AP	Displays he wireless Access Point (AP) for this asset profile.
Wireless SSID	Displays the wireless Service Set Identifier (SSID) for this asset profile.
CVSS Confidentiality Requirements	Displays the impact on confidentiality of a successfully exploited vulnerability on this asset. Options include: • Low • Medium • High • Not defined
Switch ID	Displays the switch ID for this asset profile.
Switch Port ID	Displays the switch port ID for this asset profile.

Table 8-8 Asset Summary pane parameters (continued)

Parameter	Description
CVSS Integrity Requirements	Displays the impact to the asset's integrity when a vulnerability is successfully exploited. Options include: • Low • Medium • High • Not defined
Technical User	Specifies the QRadar Log Manager user name associated with this asset profile.
Open Services	Displays the number of unique Layer 7 applications that run on this asset profile.
Vulnerabilities	Displays the number of vulnerabilities discovered on this asset profile.
Location	Specifies the physical location of the asset. By default, this field is empty. To provide a location for the asset, edit the asset profile.
Asset Description	Specifies a description for this asset. By default, this field is empty. To provide a description for the asset, edit the asset profile.
Extra Data	Specifies any extended information based on an event.

Network Interface Summary pane

The Network Interface Summary pane on the Asset Profile page provides the following information:

Table 8-9 Network Interface Summary pane parameters

Parameter	Description
MAC Address	Displays the MAC address of this asset, if known.
IP Address	Displays the IP address detected for this MAC address.
Network	Displays the network the IP address is associated with, if known.
Last Seen	Displays the date and time the IP address was last detected on this MAC address.

Vulnerability pane

The Vulnerability pane on the Asset Profile page provides the following information:

Table 8-10 Vulnerability pane parameters

Parameter	Description
ID	Displays the ID of the vulnerability. The ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Severity	Displays the Payment Security Industry (PCI) severity associated to vulnerability.

Table 8-10 Vulnerability pane parameters (continued)

Parameter	Description
Risk	Risk level associated to vulnerability. Sorting on this column must be by the underlying risk level code
Service	Service associated to the vulnerability (as discovered by scan). If only one service is associated, then display the service. Otherwise display Multiple (N) where N indicates to total number of service associated to this vulnerability.
Port	Displays the port number this vulnerability was discovered on. If the vulnerability was discovered on more than one port, this field indicates the number of port numbers. Move your mouse pointer over the value to view a list of port numbers.
Vulnerability	Name or title of this vulnerability.
Details	Specific detailed text associated to this vulnerability as determined by scan. If only one Detail is associated, then display the text of this Detail. Otherwise display Multiple (N) where N indicates to total number of Details associated to this vulnerability.
CVSS Score	Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. The CVSS score is calculated using the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see **Adding or editing an asset profile**. For more information on CVSS, see *http://www.first.org/cvss/*.
Found	Displays the date when this vulnerability was originally found in a scan.
Last seen	Displays the date when this vulnerability was last seen in a scan.

Services pane

The Services pane on the Asset Profile page provides the following information:

Table 8-11 Services pane parameters

Parameter	Description
Service	Displays the name of the open service.
Product	Displays the product that runs on this service, if known.

Table 8-11 Services pane parameters (continued)

Parameter	Description
Port	Displays the port the Layer 7 application was discovered on. If this service has more than one port, this field indicates the number of ports. Move your mouse pointer over the value to view a list of port numbers.
Protocol	Displays a comma-separated list of protocols discovered on the port that runs the open service.
Last Seen Passive	Displays the date and time that the open service was last passively seen.
Last Seen Active	Displays the date and time that the open service was last actively seen.
Service Default Ports	Displays a comma-separated list of known ports the Layer 7 application is known to run on.
Vulnerabilities	Displays the number of vulnerabilities associated with this open service.

Windows Services pane

The Windows Services pane is displayed only when QRadar Vulnerability Manager is installed on your system. The Windows Services pane on the Asset Profile page provides the following information:

Table 8-12 Windows Services pane parameters

Parameter	Description
Name	Displays the name of the Windows service that was actively seen on the asset.
Status	Displays the status of the Windows service. Options include: • Enabled • Manual • Disabled

Packages pane

The Packages pane is displayed only when QRadar Vulnerability Manager is installed on your system.The Packages pane on the Asset Profile page provides the following information:

Table 8-13 Packages pane parameters

Parameter	Description
Packages	Displays the name of the package applied to the asset.
Version	Displays the version of the package applied to the asset.
Revision	Displays the revision of the package applied to the asset.

Windows Patches pane

The Windows Patches pane is displayed only when QRadar Vulnerability Manager is installed on your system.The Windows Patches pane on the Asset Profile page provides the following information:

Table 8-14 Windows Patches pane parameters

Parameter	Description
Microsoft KB Number	Displays the Microsoft Knowledge Base (KB) number of the Windows patch that runs on the asset.
Description	Displays the description of the Windows patch.
Bulletin ID	Displays the bulletin ID number of the Windows patch.
Vulnerability ID	Displays the vulnerability ID of the Windows patch.
CVE-ID	Displays the CVE ID associated with the Windows patch. If more than one CVE ID is associated with the Windows patch, more your mouse over the Multiple link to display the list of CVE IDs. You can click a CVE ID link to access more information.
System	Displays the Windows system for the patch.
Service Pack	Displays the service pack for the patch.

Properties pane

The Properties pane is displayed only when QRadar Vulnerability Manager is installed on your system.The Properties pane on the Asset Profile page provides the following information:

Table 8-15 Properties pane parameters

Parameter	Description
Name	Displays the name of the configuration property that was actively seen on the asset.
Value	Displays the value for the configuration property.

Risk Policies pane

The Risk Policies pane is displayed only when QRadar Vulnerability Manager is installed on your system. The Risk Policies pane on the Asset Profile page provides the following information:

Table 8-16 Risk Policies pane parameters

Parameter	Description
Policy	Displays the name of the policy associated with this asset.
Pass/Fail	Indicates whether the policy has a status of **Pass** or **Fail**.
Last Evaluated	Displays the date this policy was last evaluated.

Products pane

The Products pane on the Asset Profile page provides the following information:

Table 8-17 Products pane parameters

Parameter	Description
Product	Displays the name of the product that runs on the asset.
Port	Displays the port the product uses.

Table 8-17 Products pane parameters (continued)

Parameter	Description
Vulnerability	Displays the number of vulnerabilities associated with this product.
Vulnerability ID	Displays the vulnerability ID.

9 REPORTS MANAGEMENT

You can use the **Reports** tab to create, edit, distribute, and manage reports.

The **Reports** tab provides you with:

- Detailed reporting options required to satisfy various regulatory standards, such as PCI compliance.
- Flexibility in layout and content.

Reports tab overview

You can create your own custom reports in IBM Security QRadar Log Manager or use a default reports. You can customize and rebrand default reports and distribute these to other QRadar Log Manager users.

The **Reports** tab might require an extended period of time to refresh if your system includes a large number of reports.

Note: If you are running Microsoft® Exchange Server 5.5, unavailable font characters might be displayed in the subject line of emailed reports. To resolve this, download and install Service Pack 4 of Microsoft Exchange Server 5.5. For more information, contact Microsoft support.

Timezone considerations

To ensure that the Reports feature uses the correct date and time for reporting data, your QRadar Log Manager session must be synchronized with your timezone. During the installation and setup of QRadar Log Manager, the time zone is configured. Check with your administrator to ensure your QRadar Log Manager session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports created by other QRadar Log Manager users. Non-administrative users can only view reports they created or reports which are shared by other users.

Reports tab parameters

The **Reports** tab displays a list of default and custom reports. From the **Reports** tab, you can view statistical information about the reports template, perform actions on the report templates, view the generated reports, delete generated content.

The **Reports** tab provides the following information:

Table 9-1 Reports tab parameters

Parameters	Description
Flag Column	If an error occurred, causing the report generation to fail, the **Error** icon is displayed in this column.
Report Name	Specifies the report name.
Group	Specifies the group to which this report belongs.
Schedule	Specifies the frequency with which the report is generated. Reports that specify an interval schedule, when enabled, are automatically generated according to the specified interval. If a report does not specify an interval schedule, you must manually generate the report. See **Manually generating a report**.
Next Run Time	Specifies the duration of time, in hours and minutes, until the next report is generated.
Last Modification	Specifies the last date this report was modified.
Owner	Specifies the QRadar Log Manager user that owns the report.
Author	Specifies the QRadar Log Manager user that created the report.
Generated Reports	From this list box, select the date stamp of the generated report you want to view. When you select the date stamp, the **Format** parameter displays the available formats for the generated reports. See **Viewing generated reports**. If no reports have been generated, **None** is displayed.
Formats	Specifies the report formats of the currently selected report in the **Generated Reports** column. Click the icon for the format you want to view. Report formats include: • **PDF** - Portable Document Format • **HTML** - Hyper Text Markup Language format • **RTF** - Rich Text Format • **XML** - Extensible Markup Language (only available for tables) • **XLS** - Microsoft® Excel format (only available for tables)

You can point your mouse over any report to preview a report summary in a tooltip. The summary specifies the report configuration and the type of content the report generates.

Report tab sort order

By default, reports are sorted by the **Last Modification** column. On the Reports navigation menu, reports are sorted by interval schedule. To filter the report to only display reports of a specific frequency, click the arrow beside the **Report** menu item on the navigation menu and select the group (frequency) folder.

Reports tab toolbar

You can use the toolbar to perform a number of actions on reports. The following table identifies and describes the Reports toolbar options.

Table 9-2 Reports tab toolbar options

Option	Description
Group	From the list box, select the group you want to view. The group is displayed with the assigned reports. For more information, see **Report groups**.
Manage Groups	Click **Manage Groups** to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups. For more information, see **Report groups**.
Actions	Click **Actions** to perform the following actions: • **Create** - Select this option to create a new report. For more information, see **Editing a report**. • **Edit** - Select this option to edit the selected report. You can also double-click a report to edit the content. • **Duplicate** - Select this option to duplicate or rename the selected report. For more information, see **Duplicating a report**. • **Assign Groups** - Select this option to assign the selected report to a report group. For more information, see **Report groups**. • **Share** - Select this option to share the selected report with other users. You must have administrative privileges to share reports. For more information, see **Sharing a report**. • **Toggle Scheduling** - Select this option to toggle the selected report to the Active or Inactive state. • **Run Report** - Select this option to generate the selected report. For more information, see **Manually generating a report**. To generate multiple reports, hold the Control key and click on the reports you want to generate. • **Run Report on Raw Data** - Select this option to generate the selected report using raw data. This option is useful when you want to generate a report before the required accumulated data is available. For example, if you want to run a weekly report before a full week has elapsed since you created the report, you can generate the report using this option. • **Delete Report** - Select this option to delete the selected report. To delete multiple reports, hold the Control key and click on the reports you want to delete. • **Delete Generated Content** - Select this option to delete all generated content for the selected rows. To delete multiple generated reports, hold the Control key and click on the generate reports you want to delete.

Table 9-2 Reports tab toolbar options (continued)

Option	Description
Hide Inactive Reports	Select this check box to hide inactive report templates. The **Reports** tab automatically refreshes and displays only active reports. Clear the check box to show the hidden inactive reports.
Search Reports	Type your search criteria in the **Search Reports** field and click the **Search Reports** icon. A search is run on the following parameters to determine which match your specified criteria: • Report Title • Report Description • Report Groups • Report Author User Name

Status bar

The status bar displays the number of search results (**Displaying 1 of 10 items**) currently displayed and the amount of time (**Elapsed time:**) required to process the search results.

Report layout

A report can consist of several data elements and can represent network and security data in a variety of styles, such as tables, line charts, pie charts, and bar charts.

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays a large number of objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data. To preview how each chart displays a data, see **Graph types**.

Chart types

When you create a report, you must choose a chart type for each chart you want to include in your report. The chart type determines how the generated report presents data and network objects. You can chart data with several characteristics and create the charts in a single generated report.

QRadar Log Manager includes the following chart types:

- **None** - When you select the **None** option, the container is displayed empty in the report. This option might be useful for creating white space in your report. If you select the None option for any container, no further configuration is required for that container.
- **Events/Logs** - You can use the Event/Logs chart to view event information. You can base your charts on data from saved searches from the **Log Activity** tab. This allows you to customize the data that you want to display in the generated report. You can configure the chart to plot data over a configurable period of time. This functionality helps you to detect event trends.

  For more information about saved searches, see **Data searches**.

For more information on these chart types, see **Event/Logs chart container parameter**.

Graph types

Each chart type supports a variety of graph types you can use to display data. The network configuration files determine the colors the charts use to depict network traffic. Each IP address is depicted using a unique color.

The following graph types are available for QRadar Log Manager reports:

- Line Graph
- Stacked Line Graph
- Bar Graph
- Stacked Bar Graph
- Pie Graph
- Table Graph

To display content in a table, you must design a report with a full page width container.

Creating custom reports

On the **Reports** tab, you can access the Report Wizard to create a new report.

About this task

The Report Wizard provides a step-by-step guide on how to design, schedule, and generate reports. The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder for the featured content
- **Content** - Definition of the chart that is placed in the container

After creating a report that generates weekly or monthly, the scheduled time must have elapsed before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires 7 days to build the data. This search does not return results before 7 days has elapsed.

When you specify the output format for the report, consider that the file size of generated reports can be one to two megabytes, depending on the selected output format. PDF format is smaller in size and does not consume a large quantity of disk storage space.

Procedure

Step 1 Click the **Reports** tab.

Step 2 From the **Actions** list box, select **Create**.

Step 3 On the Welcome to the Report Wizard change, click **Next** to move to the next page of the Report Wizard.

Step 4 Select one of the following scheduling options:

Option	**Description**
Manually	Generates a report once. This is the default setting; however, you can generate this report as often as required.
Hourly	Schedules the report to generate at the end of each hour using the data from the previous hour. If you choose the Hourly option, further configuration is required. From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m for both the **From** and **To** fields.
Daily	Schedules the report to generate daily using the data from the previous day. For each chart on a report, you can select the previous 24 hours of the day, or select a specific time frame from the previous day. If you choose the **Daily** option, further configuration is required. Select the check box beside each day you want to generate a report. Also, you can use the list box to select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	Schedules the report to generate weekly using the data from the previous week. If you choose the **Weekly** option, further configuration is required. Select the day you want to generate the report. The default is Monday. From the list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Monthly	Schedules the report to generate monthly using the data from the previous month. If you choose the **Monthly** option, further configuration is required. From the list box, select the date you want to generate the report. The default is the first day of the month. Also, use the list box to select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

Step 5 In the Allow this report to generate manually pane, select one of the following options and then click **Next**:

- **Yes** - Enables manual generation of this report.
- **No** - Disables manual generation of this report.

Step 6 Configure the layout of your report:

a From the **Orientation** list box, select the page orientation: Portrait or Landscape. The default is Landscape.

b Select one of the six layout options displayed on the Report Wizard.

c Click **Next** to move to the next page of the Report Wizard.

Step 7 Specify values for the following parameters:

- **Report Title** - Type a report title. The title can be up to 100 characters in length. Do not use special characters.
- **Logo** - From the list box, select a logo. For more information about branding your report, see **Branding reports**.

Step 8 Configure each container in the report:

a From the **Chart Type** list box, select a chart type. See **Chart types**.

b On the Container Details - <chart_type> window, configure the chart parameters. For detailed information about configuring your chart, see **Event/Logs chart container parameter**.

c Click **Save Container Details**.

The Wizard returns to the Specify Report Contents page, enabling you to configure the other containers in your report.

d If required, repeat steps **a** to **c** for all containers.

e Click **Next** to move to the next page of the Report Wizard.

Step 9 Preview the Layout Preview page, and then click **Next** to move to the next step of the Report Wizard.

Step 10 Select the check boxes for the report formats you want to generate, and then click **Next**.

Options include the following report formats:

- **PDF** - Portable Document Format
- **HTML** - Hyper Text Markup Language format
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (only available for tables)
- **XLS** - Microsoft® Excel format

Step 11 Select the distribution channels for your report, and then click **Next**. Options include the following distribution channels:

Option	Description
Report Console	Select this check box to send the generated report to the **Reports** tab. This is the default distribution channel.
Select the users that should be able to view the generated report.	This option is only displayed after you select the **Report Console** check box. From the list of users, select the QRadar Log Manager users you want to grant permission to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar Log Manager Administration Guide.*

Option	Description
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all QRadar Log Manager users to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar Log Manager Administration Guide.*
Email	Select this check box if you want to distribute the generated report using email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter is 255. ***Note:*** *Email recipients receive this email from no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **Email** check box. Select this check box to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the **Email** check box. Select this check box to include a link the Report Console in the email.

Step 12 On the Finishing Up page, enter values for the following parameters:

Parameter	Description
Report Description	Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.
Groups	Select the groups to which you want to assign this report. For more information about groups, see **Report groups**.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

Step 13 Click **Next** to view the report summary.

Step 14 On the Report Summary page, select the tabs available on the summary report to preview your report configuration.

Step 15 Click **Finish**.

Result

The report immediately generates. If you cleared the **Would you like to run the report now?** check box on the final page of the wizard, the report is saved and generates at the scheduled time.

The report title is the default title for the generated report. If you re-configure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Report management tasks

Using the Reports tab and the Reports Wizard, you can manage your reports. You can edit, duplicate, share, and brand reports. You can also delete generated reports.

Editing a report

Using the Report Wizard, you can edit any default or custom report to change.

About this task

QRadar Log Manager provides a significant number of default reports that you can use or customize. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Double-click the report you want to customize.

Step 3 On the Report Wizard, change the parameters to customize the report to generate the content you require. For more information on how to use the Report Wizard, see **Creating custom reports**.

Step 4 Click **Finish**.

Result

If you re-configure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Viewing generated reports

On the **Reports** tab, an icon is displayed in the **Formats** column if a report has generated content. You can click the icon to view the report.

About this task

When a report has generated content, the **Generated Reports** column displays a list box. The list box displays all generated content, organized by the time-stamp of the report. The most recent reports are displayed at the top of the list. If a report has no generated content, the **None** value is displayed in the **Generated Reports** column.

Icons representing the report format of the generated report are displayed in the **Formats** column. Reports can be generated in the following formats:

- **PDF** - Portable Document Format

- **HTML** - Hyper Text Markup Language format
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (only available for tables)
- **XLS** - Microsoft® Excel format

The XML and XLS formats are available only for reports that use a single chart table format (portrait or landscape).

You can view only the reports to which you have been given access from the QRadar Log Manager administrator. Administrative users can access all reports.

If you use the Mozilla Firefox web browser and you select the RTF report format, the Mozilla Firefox web browser launches a new browser window. This new window launch is the result of the Mozilla Firefox web browser configuration and does not affect QRadar Log Manager. You can close the window and continue with your QRadar Log Manager session.

Procedure

Step 1 Click the **Reports** tab.

Step 2 From the list box in the **Generated Reports** column, select the time-stamp of report you want to view.

Step 3 Click the icon for the format you want to view.

Result

The report opens in the selected format.

Deleting generated content

When you delete generated content, all reports that have generated from the report template are deleted, but the report template is retained.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the reports for which you want to delete the generated content.

Step 3 From the **Actions** list box, click **Delete Generated Content**.

Result

All generated content for the selected report is deleted.

Manually generating a report

A report can be configured to generate automatically, however, you can manually generate a report at any time.

About this task

While a report generates, the **Next Run Time** column displays one of the three following messages:

- **Generating** - The report is generating.

- **Queued (*position in the queue*)** - The report is queued for generation. The message indicates the position the report is in the queue. For example, 1 of 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

You can select the **Refresh** icon to refresh the view, including the information in the **Next Run Time** column.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to generate.

Step 3 Click **Run Report**.

What to do next

After the report generates, you can view the generated report from the **Generated Reports** column. See **Viewing generated reports**.

Duplicating a report

To create a report that closely resembles an existing report, you can duplicate the report you want to model, and then customize it.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to duplicate.

Step 3 From the **Actions** list box, click **Duplicate**.

Step 4 Type a new name, without spaces, for the report.

Step 5 Click **OK**.

The new report is displayed in the reports list.

What to do next

You can customize the duplicated report. See **Editing a report**.

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule.

About this task

Any updates that the user makes to a shared report does not affect the original version of the report.

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the reports you want to share.

Step 3 From the **Actions** list box, click **Share**.

Step 4 From the list of users, select the users with whom you want to share this report.

If no users with appropriate access are available, a message is displayed.

Step 5 Click **Share**.

Branding reports

To brand reports, you can import logos and specific images. To brand reports with custom logos, you must upload and configure the logos before you begin using the Report Wizard.

Before you begin

Ensure that the graphic you want to use is 144 x 50 pixels with a white background.

To make sure your browser displays the new logo, clear your browser cache.

About this task

Report branding is beneficial for your enterprise if you support more than one logo. When you upload an image to QRadar Log Manager, the image is automatically saved as a Portable Network Graphic (PNG).

When you upload a new image and set the image as your default, the new default image is not applied to reports that have been previously generated. Updating the logo on previously generated reports requires you to manually generate new content from the report.

If you upload an image that is larger in length than the report header can support, the image automatically resizes to fit the header; this is approximately 50 pixels in height.

Procedure

Step 1 Click the **Reports** tab.

Step 2 On the navigation menu, click **Branding**.

Step 3 Click **Browse** to browse the files located on your system.

Step 4 Select the file that contains the logo you want to upload.

Step 5 Click **Open**.

Step 6 Click **Upload Image** to upload the image to QRadar Log Manager.

Step 7 Select the logo you want to use as the default and click **Set Default Image**.

Report groups

On the **Reports** tab, you can sort the list of reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports. For example, you can view all reports related to Payment Card Industry Data Security Standard (PCIDSS) compliance.

By default, the **Reports** tab displays the list of all reports, however, you can categorize reports into groups such as:

- Compliance
- Executive
- Log Sources
- Network Management
- Security
- VoIP
- Other

When you create a new report, you can assign the report to an existing group or create a new group. You must have administrative access to create, edit, or delete groups. For more information about user roles, see the *IBM Security QRadar Log Manager Administration Guide*.

Creating a group

QRadar Log Manager includes default report groups, however, you can also add groups.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 Using the navigation tree, select the group under which you want to create a new group.

Step 4 Click **New Group**.

Step 5 Enter values for the following parameters:

- **Name** - Type the name for the new group. The name can be up to 255 characters in length.
- **Description** - Type a description for this group. The description can be up to 255 characters in length. This field is optional.

Step 6 Click **OK**.

Step 7 To change the location of the new group, click the new group and drag the folder to the new location on the navigation tree.

Step 8 Close the Report Groups window.

Editing a group

You can edit a report group to change the name or description.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, select the group you want to edit.

Step 4 Click **Edit**.

Step 5 Update values for the parameters, as necessary:

- **Name** - Type the name for the new group. The name can be up to 255 characters in length.
- **Description** - Type a description for this group. The description can be up to 255 characters in length. This field is optional.

Step 6 Click **OK**.

Step 7 Close the Report Groups window.

Assigning a report to a group

Using the **Assign Groups** option, you can assign a report to a another group.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to assign to a group.

Step 3 From the **Actions** list box, select **Assign Groups**.

Step 4 From the **Item Groups** list, select the check box of the group you want to assign to this report.

Step 5 Click **Assign Groups**.

Copying a report to another group

Using the **Copy** icon, you can copy a report to one or more report groups.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, select the report you want to copy.

Step 4 Click **Copy**.

Step 5 Select the group or groups to which you want to copy the report.

Step 6 Click **Assign Groups**.

Step 7 Close the Report Groups window.

Removing a report from a group

Using the **Remove** icon, you can remove a report from a group.

About this task

When you remove a report from a group, the report still exists on the **Reports** tab. The report is not removed from your system.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, navigate to the folder that contains the report you want to remove.

Step 4 From the list of groups, select the report you want to remove.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Report Groups window.

Event/Logs chart container parameter

The following table describes the Events/Logs chart container parameters:

Table 9-3 Event/Logs chart container parameters

Parameter	Description
Container Details - Events/Logs	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Events/Logs to Top	From the list box, select the number of events/logs to be displayed in the generated report.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Bar** - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search. • **Line** - Displays the data in a line chart. • **Pie** - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search. • **Stacked Bar** - Displays the data in a stacked bar chart. • **Stacked Line** - Displays the data in a stacked line chart. • **Table** - Displays the data in table format. The **Table** option is only available for the full page width container only. To view examples of each graph charts data type, see **Graph types**.

Table 9-3 Event/Logs chart container parameters (continued)

Parameter	Description
Manual Scheduling	The Manual Scheduling pane is displayed only if you selected the **Manually** scheduling option in the Report Wizard. Using the Manual Scheduling options, you can create a manual schedule that can run a report over a custom defined period of time, with the option to only include data from the hours and days that you select. For example, you can schedule a report to run from October 1 to October 31, only including data generated during your business hours, such as Monday to Friday, 8 AM to 9 PM. To create a manual schedule: **1** From the **From** list box, type the start date you want for the report, or select the date using the **Calender** icon. The default is the current date. **2** From the list boxes, select the start time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **3** From the **To** list box, type the end date you want for the report, or select the date using the **Calender** icon. The default is the current date. **4** From the list boxes, select the end time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **5** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the* ***Timezone*** *parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as* ***GMT -5.00 America/New_York****, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 9-3 Event/Logs chart container parameters (continued)

Parameter	**Description**
Hourly Scheduling	The Hourly Scheduling pane is displayed only if you selected the **Hourly** scheduling option in the Report Wizard. ▶ From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* Hourly Scheduling automatically graphs all data from the previous hour.
Daily Scheduling	The Daily Scheduling pane is displayed only if you selected the **Daily** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous day (24 hours)** • **Data of previous day from** - From the list boxes, select the period of time you want for the generated report. Time is available in half-hour increments. The default is 1:00 a.m. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.*

Table 9-3 Event/Logs chart container parameters (continued)

Parameter	Description
Weekly Scheduling	The Weekly Scheduling pane is displayed only if you selected the **Weekly** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous week** • **All Data from previous week from** - From the list boxes, select the period of time you want for the generated report. The default is Sunday. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 9-3 Event/Logs chart container parameters (continued)

Parameter	**Description**
Monthly Scheduling	The Monthly Scheduling pane is displayed only if you selected the **Monthly** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous month** • **Data from previous month from the** - From the list boxes, select the period of time you want for the generated report. The default is 1st to 31st. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.
Graph Content	
Group	From the list box, select a saved search group to display the saved searches belonging to that group in the **Available Saved Searches** list box.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type `Firewall` to display a list of all searches that include Firewall in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed, however, you can filter the list by selecting a group from the **Group** list box or typing the name of a known saved search in the **Type Saved Search or Select from List** field.

Table 9-3 Event/Logs chart container parameters (continued)

Parameter	Description
Create New Event Search	Click **Create New Event Search** to create a new search. For more information about how to create an event search, see **Log activity investigation**.

A DEFAULT RULES AND BUILDING BLOCKS

The Enterprise template includes settings with emphasis on internal network activities.

Default rules

Default rules for the Enterprise template include:

Table 10-1 Default rules

Rule	Group	Rule type	Enabled	Description
Anomaly: Devices with High Event Rates	Anomaly	Event	False	Monitors devices for high event rates. Typically, the default threshold is low for most networks and we recommend that you adjust this value before enabling this rule. To configure which devices will be monitored, edit the BB:DeviceDefinition: Devices to Monitor for High Event Rates BB.
Anomaly: DMZ Jumping	Anomaly	Common	False	Reports when connections are bridged across your Demilitarized Zone (DMZ).
Anomaly: DMZ Reverse Tunnel	Anomaly	Common	False	Reports when connections are bridged across your DMZ through a reverse tunnel.
Anomaly: Excessive Database Connections	Anomaly	Event	True	Reports an excessive number of successful database connections.
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Anomaly	Event	False	Reports excessive firewall accepts across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.
Anomaly: Excessive Firewall Accepts Across Multiple Sources to a Single Destination	Anomaly	Event	False	Reports excessive firewall accepts from multiple hosts to a single destination. Detects more than 100 firewall accepts across more than 100 sources IP addresses within 5 minutes.
Anomaly: Excessive Firewall Denies from Single Source	Anomaly	Event	True	Reports excessive firewall denies from a single host. Detects more than 400 firewall deny attempts from a single source to a single destination within 5 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Anomaly: Outbound Connection to a Foreign Country/Region	Anomaly	Event	False	Reports successful logins or access from an IP address known to be in a country or region that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries/Regions with no Remote Access BB.
Anomaly: Potential Honeypot Access	Anomaly	Event	False	Reports an event that has a source or destination IP address defined as a honeypot or tarpit address. Before enabling this rule, you must configure the BB:HostDefinition: Honeypot like addresses BB.
Anomaly: Remote Access from Foreign Country/Region	Anomaly	Event	False	Reports successful logins or access from an IP address known to be in a country or region that does not have remote access right. Before you enable this rule, we recommend that you configure the BB:CategoryDefinition: Countries/Regions with no Remote Access BB.
Anomaly: Single IP with Multiple MAC Addresses	Anomaly	Event	False	Reports when the MAC address of a single IP address changes multiple times over a period of time.
Anomaly: Systems using many different protocols	Anomaly	Common	False	Reports when a local systems connects to the Internet on more than 50 destination ports over a one-hour period.
Authentication: Login Failure to Disabled Account	Authentication	Event	False	Reports a host login failure message from a disabled user account. If the user is no longer a member of your organization, we recommend that you investigate other received authentication messages from the same user.
Authentication: Login Failure to Expired Account	Authentication	Event	False	Reports a host login failure message from an expired user account known. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages from the same user.
Authentication: Login Failures Followed By Success to the same Destination IP	Authentication	Event	True	Reports multiple login failures to a single destination IP address, followed by a successful login to the destination IP address.
Authentication: Login Failures Followed By Success From Single Source IP	Authentication	Event	True	Reports multiple login failures from a single source IP address, followed by a successful login.
Authentication: Login Failures Followed By Success to the same Username	Authentication	Event	True	Reports multiple login failures followed by a successful login from the same user.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Authentication: Login Successful After Scan Attempt	Authentication	Common	True	Reports a successful login to a host after reconnaissance has been detected on this network.
Authentication: Multiple Login Failures for Single Username	Authentication	Event	True	Reports authentication failures for the same user name.
Authentication: Multiple Login Failures from the Same Source	Authentication	Event	True	Reports authentication failures from the same source IP address to more than three destination IP address more than ten times within 5 minutes.
Authentication: Multiple Login Failures from the Same Source (Windows)	Authentication	Event	False	Reports authentication failures from the same Windows source IP address to more than three destination IP address more than ten times within 5 minutes.
Authentication: Multiple Login Failures to the Same Destination	Authentication	Event	True	Reports authentication failures to the same destination IP address from more than ten source IP addresses more than ten times within 10 minutes.
Authentication: Multiple VoIP Login Failures	Authentication	Event	False	Reports multiple login failures to a VoIP PBX host.
Authentication: No Activity for 60 Days	Authentication	Event	False	Reports when the configured users have not logged in to the host for over 60 days
Authentication: Possible Shared Accounts	Authentication	Event	False	Reports when an account is shared. We recommend that you add system accounts, such as root and admin to the following negative test: and NOT when the event user name matches the following.
Authentication: Repeat Non-Windows Login Failures	Authentication	Event	False	Reports when a source IP address causes an authentication failure event at least seven times to a single destination IP address within 5 minutes.
Authentication: Repeat Windows Login Failures	Authentication	Event	False	Reports when a source IP address causes an authentication failure event at least nine times to a single Windows host within 1 minute.
Botnet: Local Host on Botnet CandC List (SRC)	Botnet	Common	True	Reports when a source IP address is a member of a known Botnet CandC host.
Botnet: Local host on Botnet CandC List (DST)	Botnet	Common	True	Reports when a local destination IP address is a member of a known Botnet CandC host.
Botnet: Potential Botnet Connection (DNS)	Botnet	Common	False	Reports a host connecting or attempting to connect to a DNS server on the Internet. This might indicate a host connecting to a Botnet.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Botnet: Potential connection to known Botnet CandC	Botnet	Common	True	Reports when a potential connection to a know BotNet CandC host is detected. To reduce false positive events, connections on ports 25 and 53 are removed from the rule.
Botnet: Successful Inbound Connection from a Known Botnet CandC	Botnet	Common	True	Reports when a successful inbound connection from a BotNet CandC host in detected.
Policy: Remote: IRC Connections	Botnet, Policy	Common	True	Reports a local host issuing an excessive number of IRC connections to the Internet.
Compliance: Auditing Services Stopped on Compliance Host	Compliance	Event	False	Reports when auditing services are stopped on a compliance host. Before enabling this rule, define the hosts in the compliance definition BBs and verify that the events for the audit service stopped for your host are in the BB: CategoryDefinition: Auditing Stopped building block.
Compliance: Configuration Change Made to Device in Compliance network	Compliance	Event	False	Reports configuration change made to device in compliance network. Before you enable this rule, edit the device list to include the devices you want reported.
Compliance: Excessive Failed Logins to Compliance IS	Compliance	Event	False	Reports excessive authentication failures to a compliance server within 10 minutes.
Compliance: Traffic from DMZ to Internal Network	Compliance	Common	True	Reports traffic from the DMZ to an internal network. This is typically not allowed under compliance regulations. Before enabling this rule, make sure the DMZ object is defined in your network hierarchy.
Compliance: Traffic from Untrusted Network to Trusted Network	Compliance	Common	True	Reports traffic from an untrusted network to a trusted network. Before enabling this rule, edit the following BBs: BB:NetworkDefinition: Untrusted Network Segment and BB:NetworkDefinition: Trusted Network Segment.
Database: Attempted Configuration Modification by a remote host	Compliance	Event	True	Reports when a configuration modification is attempted to a database server from a remote network.
Database: Concurrent Logins from Multiple Locations	Compliance	Event	True	Reports when several authentications to a database server occur across multiple remote IP addresses.
Database: Attempted Configuration Modification by a remote host	Database	Event	True	Reports when a configuration modification is attempted to a database server from a remote network.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Database: Concurrent Logins from Multiple Locations	Database	Event	True	Reports when multiple remote IP addresses concurrently login to a database server.
Database: Failures Followed by User Changes	Database	Event	True	Reports when login failures are followed by the addition or change of a user account.
Database: Groups changed from Remote Host	Database	Event	True	Monitors changes to groups on a database when the change is initiated from a remote network.
Database: Multiple Database Failures Followed by Success	Database	Event	True	Reports when there are multiple database failures followed by a success within a short period of time.
Database: Remote Login Failure	Database	Event	True	Reports when a login failure from a remote source IP address to a database server is detected.
Database: Remote Login Success	Database	Event	True	Reports when a successful authentication occurs to a database server from a remote network.
Database: User Rights Changed from Remote Host	Database	Event	True	Reports when changes to database user privileges are made from a remote network.
DDoS: DDoS Attack Detected	D\DoS	Event	True	Reports network Distributed Denial of Service (DDoS) attacks on a system.
DoS: DoS Events from Darknet	D/DoS	Event	False	Reports when DoS attack events are identified on Darknet network ranges.
DoS: Network DoS Attack Detected	D\DoS	Event	True	Reports network Denial of Service (DoS) attacks on a system.
DoS: Service DoS Attack Detected	D\DoS	Event	True	Reports a DoS attack against a local destination IP address that is known to exist and the target port is open.
Botnet: Potential Botnet Connection (DNS)	Exploit	Common	False	Reports a host connecting or attempting to connect to a DNS server on the Internet. This might indicate a host connecting to a Botnet. The host should be investigated for malicious code. Before you enable this rule, configure the BB:HostDefinition: DNS Servers BB. ***Note:*** *Notebooks that include wireless adapters might cause this rule to generate alerts since the laptops might attempt to communicate with another IDPs DNS server. If this occurs, define the ISPs DNS server in the BB:HostDefinition: DNS Servers BB.*
Exploit: Attack followed by Attack Response	Exploit	Event	False	Reports when exploit events are followed by typical responses, which might indicate a successful exploit.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Exploit: Chained Exploit Followed by Suspicious Events	Exploit	Event	True	Reports exploit activity from a source IP address followed by suspicious account activity to a third host from the same destination IP address as the original exploit within 15 minutes.
Exploit: Destination Vulnerable to Detected Exploit	Exploit	Event	True	Reports an exploit against a vulnerable local destination IP address, where the destination IP address is known to exist, and the host is vulnerable to the exploit.
Exploit: Destination Vulnerable to Detected Exploit on a Different Port	Exploit	Event	True	Reports an exploit against a vulnerable local destination IP address, where the destination IP address is known to exist, and the host is vulnerable to the exploit on a different port.
Exploit: Destination Vulnerable to Different Exploit than Attempted on Targeted Port	Exploit	Event	False	Reports an exploit against a vulnerable local destination IP address, where the target is known to exist, and the host is vulnerable to some exploit but not the one being attempted.
Exploit: Exploit Followed by Suspicious Host Activity	Exploit	Event	False	Reports an exploit from a source IP address followed by suspicious account activity on the destination host within 15 minutes.
Exploit: Exploit/Malware Events Across Multiple Destinations	Exploit	Event	True	Reports a source IP address generating multiple (at least five) exploits or malicious software (malware) events in the last 5 minutes. These events are not targeting hosts that are vulnerable and might indicate false positives generating from a device.
Exploit: Exploits Followed by Firewall Accepts	Exploit	Event	False	Reports when exploit events are followed by firewall accept events, which might indicate a successful exploit.
Exploit: Multiple Exploit Types Against Single Destination	Exploit	Event	True	Reports a destination IP address being exploited using multiple types of exploit types from one or more source IP address.
Exploit: Multiple Vector Attack Source	Exploit	Event	False	Reports when a source IP address attempts multiple attack vectors. This might indicate a source IP address specifically targeting an asset.
Exploit: Potential VoIP Toll Fraud	Exploit	Event	False	Reports when at least three failed login attempts within 30 seconds followed by sessions being opened are detected on your VoIP hardware. This action can indicate that illegal users are executing VoIP sessions on your network.
Exploit: Recon followed by Exploit	Exploit	Event	True	Reports reconnaissance events followed by an exploit from the same source IP address to the same destination port within 1 hour.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
FalsePositive: False Positive Rules and Building Blocks	False Positive	Event	True	Reports events that include false positive rules and BBs, such as, BB:FalsePositive: Windows Server False Positive Events. Events that match the rule are stored and dropped from the event pipeline. If you add any new BBs or rules to remove events from becoming events, you must add these new rules or BBs to this rule.
Magnitude Adjustment: Context is Local to Local	Magnitude Adjustment	Common	True	Adjusts the relevance of events when there is local to local communication
Magnitude Adjustment: Context is Local to Remote	Magnitude Adjustment	Common	True	Adjusts the relevance of events when there is local to remote communication.
Magnitude Adjustment: Context is Remote to Local	Magnitude Adjustment	Common	True	Adjusts the relevance of events when there is remote to local communication.
Magnitude Adjustment: Destination Network Weight is High	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the destination network weight is high.
Magnitude Adjustment: Destination Network Weight is Low	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the destination network weight is low.
Magnitude Adjustment: Destination Network Weight is Medium	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the destination network weight is medium.
Magnitude Adjustment: Source Address is a Bogon IP	Magnitude Adjustment	Common	True	Adjusts the severity of events when the source IP is a known bogon address. Traffic from known bogon addresses might indicate the possibility of the source IP address being spoofed.
Magnitude Adjustment: Source Address is a Known Questionable IP	Magnitude Adjustment	Common	True	Adjusts the severity of events when the source IP is a known questionable host.
Magnitude Adjustment: Source Network Weight is High	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the source network weight is high.
Magnitude Adjustment: Source Network Weight is Low	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the source network weight is low.
Magnitude Adjustment: Source Network Weight is Medium	Magnitude Adjustment	Common	True	Adjusts the relevance of events if the source network weight is medium.
Malware: Local Host Sending Malware	Malware	Event	False	Reports malware being sent from local hosts.
Malware: Malware or Virus Clean Failed	Malware	Event	True	Reports when a system detected a virus and failed to clean or remove it.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Policy: Connection to a remote proxy or anonymization service	Policy	Common	True	Reports events associated with remote proxy and anonymization services.
Policy: Connection to Internet on Unauthorized Port	Policy	Common	False	Reports events connecting to the Internet on unauthorized ports.
Policy: New Host Discovered	Policy	Event	False	Reports when a new host has been discovered on the network.
Policy: New Host Discovered in DMZ	Policy	Event	False	Reports when a new host has been discovered in the DMZ.
Policy: New Service Discovered	Policy	Event	False	Reports when a new service is discovered on an existing host.
Policy: New Service Discovered in DMZ	Policy	Event	False	Reports when a new service has been discovered on an existing host in the DMZ.
Policy: Possible Local IRC Server	Policy	Common	True	Reports a local host running a service on a typical IRC port. This is not typical for enterprises and should be investigated.
Policy: Remote: IRC Connections	Policy	Common	False	Reports a local host issuing an excessive number of IRC connections to the Internet.
Policy: Upload to Local WebServer	Policy	Event	False	Reports potential file uploads to a local web server. To edit the details of this rule, edit the BB:CategoryDefinition: Upload to Local WebServer BB.
Recon: Aggressive Local L2L Scanner Detected	Recon	Common	True	Reports an aggressive scan from a local source IP address, scanning other local IP addresses. More than 400 destination IP addresses received reconnaissance or suspicious events in less than 2 minutes. This might indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm is present on the system.
Recon: Aggressive Local L2R Scanner Detected	Recon	Common	True	Reports an aggressive scan from a local source IP address, scanning remote IP addresses. More than 400 destination IP addresses received reconnaissance or suspicious events in less than 2 minutes. This might indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm is present on the system.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Aggressive Remote Scanner Detected	Recon	Common	True	Reports an aggressive scan from a remote source IP address, scanning other local or remote IP addresses. More than 50 destination IP addresses received reconnaissance or suspicious events in less than 3 minutes. This might indicate a manually driven scan, an exploited host searching for other destination IP addresses, or a worm on a system.
Recon: Excessive Firewall Denies From Local Hosts	Recon	Common	True	Reports excessive attempts, from local hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Recon: Excessive Firewall Denies From Remote Hosts	Recon	Common	True	Reports excessive attempts, from remote hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Recon: Host Port Scan Detected by Remote Host	Recon	Common	True	Reports when more than 400 ports are scanned from a single source IP address in under 2 minutes.
Recon: Local L2L LDAP Server Scanner	Recon	Common	True	Reports a source local IP address attempting reconnaissance or suspicious connections on common local LDAP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R LDAP Server Scanner	Recon	Common	True	Reports a source local IP address attempting reconnaissance or suspicious connections on common remote LDAP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Database Scanner	Recon	Common	True	Reports a scan from a local host against other local destination IP addresses. At least 30 host were scanned in 10 minutes.
Recon: Local L2R Database Scanner	Recon	Common	True	Reports a scan from a local host against remote destination IP addresses. At least 30 host were scanned in 10 minutes.
Recon: Local L2L DHCP Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local DHCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R DHCP Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote DHCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local DNS ports to more than 60 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Local L2R DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote DNS ports to more than 60 hosts in 10 minutes.
Recon: Local L2L FTP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local FTP ports to more than 30 hosts in 10 minutes.
Recon: Local L2R FTP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote FTP ports to more than 30 hosts in 10 minutes.
Recon: Local L2L Game Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local game server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Game Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote game server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L ICMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local ICMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R ICMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote ICMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L IM Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local IM server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R IM Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote IM server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L IRC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local IRC server ports to more than 10 hosts in 10 minutes.
Recon: Local L2R IRC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote IRC server ports to more than 10 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Local L2L Mail Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local mail server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Mail Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote mail server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L P2P Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local P2P server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R P2P Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote P2P server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Proxy Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local proxy server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Proxy Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote proxy server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L RPC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local RPC server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R RPC Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote RPC server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Scanner Detected	Recon	Common	True	Reports a scan from a local host against other local destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Local L2R Scanner Detected	Recon	Common	True	Reports a scan from a local host against remote destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Local L2L SNMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local SNMP ports to more than 60 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Local L2R SNMP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote SNMP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L SSH Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local SSH ports to more than 30 hosts in 10 minutes.
Recon: Local L2R SSH Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common remote SSH ports to more than 30 hosts in 10 minutes.
Recon: Local L2L Suspicious Probe Events Detected	Recon	Common	False	Reports when various suspicious or reconnaissance events have been detected from the same local source IP address to more than five local destination IP address in 4 minutes. This can indicate various forms of host probing, such as Nmap reconnaissance, which attempts to identify the services and operation systems of the host.
Recon: Local L2R Suspicious Probe Events Detected	Recon	Common	False	Reports when various suspicious or reconnaissance events have been detected from the same remote source IP address to more than five local destination IP address in 4 minutes. This can indicate various forms of host probing, such as Nmap reconnaissance, which attempts to identify the services and operation systems of the host.
Recon: Local L2L TCP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local TCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R TCP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote TCP ports to more than 60 hosts in 10 minutes.
Recon: Local L2L UDP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local UDP ports to more than 60 hosts in 10 minutes.
Recon: Local L2R UDP Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common Remote UDP ports to more than 60 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Local L2L Web Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Recon: Local L2R Web Server Scanner	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote web server ports to more than 60 hosts in 10 minutes.
Recon: Local L2L Windows Server Scanner to Internet	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common local Windows server ports to more than 60 hosts in 20 minutes.
Recon: Local L2R Windows Server Scanner to Internet	Recon	Common	True	Reports a local source IP address attempting reconnaissance or suspicious connections on common remote Windows server ports to more than 60 hosts in 20 minutes.
Recon: Local Windows Server Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common Windows server ports to more than 200 hosts in 20 minutes.
Recon: Potential Local Port Scan Detected	Recon	Common	True	Reports on potential local port scans.
Recon: Potential P2P Traffic Detected	Recon	Common	True	Reports on potential P2P traffic.
Recon: Recon Followed by Accept	Recon	Common	False	Reports when a host that has been performing reconnaissance also has a firewall accept following the reconnaissance activity.
Recon: Remote Database Scanner	Recon	Common	True	Reports a scan from a remote host against other local or remote destination IP addresses. At least 30 hosts were scanned in 10 minutes.
Recon: Remote DHCP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common DHCP ports to more than 30 hosts in 10 minutes.
Recon: Remote DNS Scanner	Recon	Common	True	Reports a source IP address attempting reconnaissance or suspicious connections on common DNS ports to more than 60 hosts in 10 minutes.
Recon: Remote FTP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common FTP ports to more than 30 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Remote Game Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common game server ports to more than 30 hosts in 10 minutes.
Recon: Remote ICMP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common ICMP ports to more than 60 hosts in 10 minutes.
Recon: Remote IM Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common IM server ports to more than 60 hosts in 10 minutes.
Recon: Remote IRC Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common IRC server ports to more than 10 hosts in 10 minutes.
Recon: Remote LDAP Server Scanner	Recon	Common	True	Reports a scan from a remote host against other local or remote destination IP addresses. At least 30 hosts were scanned in 10 minutes.
Recon: Remote Mail Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common mail server ports to more than 30 hosts in 10 minutes.
Recon: Remote Proxy Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common proxy server ports to more than 30 hosts in 10 minutes.
Recon: Remote RPC Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common RPC server ports to more than 30 hosts in 10 minutes.
Recon: Remote Scanner Detected	Recon	Common	True	Reports a scan from a remote host against other hosts or remote destination IP addresses. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Recon: Remote SNMP Scanner	Recon	Common	True	Reports a remote host scans at least 30 local or remote hosts in 10 minutes.
Recon: Remote SSH Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common SSH ports to more than 30 hosts in 10 minutes.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
Recon: Remote Suspicious Probe Events Detected	Recon	Common	False	Reports various suspicious or reconnaissance events from the same remote source IP address to more then five destination IP addresses in 4 minutes. This might indicate various forms of host probing, such as Nmap reconnaissance that attempts to identify the services and operating system of the destination IP addresses.
Recon: Remote TCP Scanner	Recon	Common	False	Reports a remote host attempting reconnaissance or suspicious connections on common TCP ports to more than 60 hosts in 10 minutes.
Recon: Remote UDP Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common UDP ports to more than 60 hosts in 10 minutes.
Recon: Remote Web Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Recon: Remote Windows Server Scanner	Recon	Common	True	Reports a remote host attempting reconnaissance or suspicious connections on common Windows server ports to more than 60 hosts in 10 minutes.
Recon: Single Merged Recon Events Local Scanner	Recon	Common	True	Reports merged reconnaissance events generated by local scanners. This rule causes all these events to create an event. All devices of this type and their event categories should be added to the BB:ReconDetected: Devices which Merge Recon into Single Events BB.
Recon: Single Merged Recon Events Remote Scanner	Recon	Common	True	Reports merged reconnaissance events generated by remote scanners. This rule causes all these events to create an event. All devices of this type and their event categories should be added to the BB:ReconDetected: Devices which Merge Recon into Single Events BB.
SuspiciousActivity: Common Non-Local to Remote Ports	Suspicious	Common	False	Rule identifies events that have common internal only ports, communicating outside of the local network.
SuspiciousActivity: Communication with Known Hostile Networks	Suspicious	Common	False	Reports events associated with known hostile networks.
SuspiciousActivity: Communication with Known Online Services	Suspicious	Common	False	Reports events associated with networks identified as websites that might involve data loss.

Table 10-1 Default rules (continued)

Rule	Group	Rule type	Enabled	Description
SuspiciousActivity: Communication with Known Watched Networks	Suspicious	Common	False	Reports events associated with networks you want to monitor.
System:Critical System Events	System	Event	False	Reports when QRadar Log Manager detects critical event.
System: Device Stopped Sending Events	System	Event	False	Reports when a log source has not sent an event to the system in over 1 hour. Edit this rule to add devices you want to monitor.
System: Device Stopped Sending Events (Firewall, IPS, VPN or Switch)	System	Event	True	Reports when a firewall, IPS, VPN or switch log source has not sent an event in over 30 minutes
System: Host Based Failures	System	Event	False	Reports when QRadar Log Manager detects events that indicate failures within services or hardware.
System: Load Building Blocks	System	Event	True	Loads the BBs required to assist with reporting. This rule has no actions or responses.
System: Multiple System Errors	System	Event	False	Reports when a source IP address has 10 system errors within 3 minutes.
System:Notification	System	Event	True	Rule ensures that notification events shall be sent to the notification framework.
System: Service Stopped and not Restarted	System	Event	False	Reports when a services has been stopped on a system and not restarted.

Default building blocks

Default building blocks for the Enterprise template include:

Table 10-2 Default building blocks

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB: CategoryDefinition: Application or Service Installed or Modified	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected when an application or service is installed or modified on a host.	
BB: CategoryDefinition: Auditing Stopped	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected when auditing has stopped on a host.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Logout Events	Category Definitions	Event	Edit this BB to include all events that indicate successful logout attempts from devices.	
BB: CategoryDefinition: Service Started	Category Definition	Event	Edit the BB to include all event categories that indicate a service has started.	
BB: CategoryDefinition: Service Stopped	Category Definition	Event	Edit the BB to include all event categories that indicate a service has stopped.	
BB: CategoryDefinition: Superuser Accounts	Category Definition	Event	Edit this BB to include user names associated with superuser accounts, such as admin, superuser, and root.	
BB: CategoryDefinition: System or Device Configuration Change	Category Definition	Event	Edit this BB is include event categories associated with system or device configuration changes.	
BB:BehaviorDefinition: Compromise Activities	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected during a typical compromise.	
BB:BehaviorDefinition: Post Compromise Activities	Category Definitions	Event	Edit this BB to include event categories that are considered part of events detected after a typical compromise.	
BB:CategoryDefinition: Access Denied	Category Definition	Event	Edit this BB to include all event categories that indicate access denied.	
BB:CategoryDefinition: Authentication Failures	Compliance	Event	Edit this BB to include all events that indicate an unsuccessful attempt to access the network.	
BB:CategoryDefinition: Authentication Success	Compliance	Event	Edit this BB to include all events that indicate successful attempts to access the network.	
BB:CategoryDefinition: Authentication to Disabled Account	Compliance	Event	Edit this BB to include all events that indicate failed attempts to access the network using a disabled account.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Authentication to Expired Account	Compliance	Event	Edit this BB to include all events that indicate failed attempts to access the network using an expired account.	
BB:CategoryDefinition: Authentication User or Group Added or Changed	Compliance	Event	Edit this BB to include all events that indicate modification to accounts or groups.	
BB:CategoryDefinition: Countries/Regions with no Remote Access	Category Definitions	Event	Edit this BB to include any geographic location that typically is not allowed remote access to the enterprise. When configured, you can enable the Anomaly: Remote Access from Foreign Country or Region rule.	
BB:CategoryDefinition: Database Access Denied	Category Definition	Event	Edit this BB to include all events that indicates denied access to the database.	
BB:CategoryDefinition: Database Access Permitted	Category Definition	Event	Edit this BB to include all events that indicates permitted access to the database.	
BB:CategoryDefinition: Database Connections	Category Definitions	Event	Edit this BB to define successful logins to databases. You might be required to add additional device types for this BB.	
BB:CategoryDefinition: DDoS Attack Events	Category Definitions	Event	Edit this BB to include all event categories that you want to categorize as a DDoS attack.	
BB:CategoryDefinition: Exploits, Backdoors, and Trojans	Category Definitions	Event	Edit this BB to include all events that are typically exploits, backdoor, or trojans.	
BB:CategoryDefinition: Failure Service or Hardware	Compliance	Event	Edit this BB that indicate failure within a service or hardware.	
BB:CategoryDefinition: Firewall or ACL Accept	Category Definitions	Event	Edit this BB to include all events that indicate access to the firewall.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Firewall or ACL Denies	Category Definitions	Event	Edit this BB to include all events that indicate unsuccessful attempts to access the firewall.	
BB:CategoryDefinition: Firewall System Errors	Category Definitions	Event	Edit this BB to include all events that might indicate a firewall system error. By default, this BB applies when an event is detected by one or more of the following devices: • Check Point • Generic Firewall • Iptables • NetScreen Firewall • Cisco Pix	
BB:CategoryDefinition: High Magnitude Events	Category Definitions	Event	Edit this BB to the severity, credibility, and relevance levels you want to generate an event. The defaults are: • Severity = 6 • Credibility = 7 • Relevance = 7	
BB:CategoryDefinition: IRC Detected Based on Event Category	Category Definitions	Event	This Building Block to include event categories that are typically associated with IRC traffic.	
BB:CategoryDefinition: IRC Detection Based on Firewall Events	Category Definitions	Event	This Building Block to include event categories and port definitions that are typically associated with IRC traffic.	BB:CategoryDefinition: Firewall or ACL Accept BB:PortDefinition: IRC Ports
BB:CategoryDefinition: KeyLoggers	Category Definitions	Event	Edit this BB to include all events associated with key logger monitoring of user activities.	
BB:CategoryDefinition: Mail Policy Violation	Compliance	Event	Edit this BB to define mail policy violations.	
BB:CategoryDefinition: Malware Annoyances	Category Definitions	Event	Edit this BB to include event categories that are typically associated with spyware infections.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Network DoS Attack	Category Definitions	Event	Edit this BB to include all event categories that you want to categorize as a network DoS attack.	
BB:CategoryDefinition: Policy Events	Compliance	Event	Edit this BB to include all event categories that might indicate a violation to network policy.	
BB:CategoryDefinition: Post DMZ Jump	Category Definitions	Event	Edit this BB to define actions that might be seen within a Remote-to-Local (R2L) and a DMZ host jumping scenario.	
BB:CategoryDefinition: Post Exploit Account Activity	Category Definitions	Event	Edit this BB to include all event categories that might indicate exploits to accounts.	
BB:CategoryDefinition: Pre DMZ Jump	Category Definitions	Event	Edit this BB to define actions that might be seen within a Local-to-Local (L2L) and a DMZ host jumping scenario.	
BB:CategoryDefinition: Pre Reverse DMZ Jump	Category Definitions	Event	Edit this BB to define actions that might be seen within a Pre DMZ jump followed by a reverse DMZ jump.	
BB:CategoryDefinition: Recon Event Categories	Category Definitions	Event	Edit this BB to include all event categories that indicate reconnaissance activity.	
BB:CategoryDefinition: Recon Events	Category Definitions	Common	Edit this BB to include all events that indicate reconnaissance activity.	
BB:CategoryDefinition: Reverse DMZ Jump	Category Definitions	Common	Edit this BB to define actions that might be seen within a Remote-to-Local (R2L) and a DMZ host reverse jumping scenario.	
BB:CategoryDefinition: Service DoS	Category Definitions	Event	Edit this BB to define Denial of Service (DoS) attack events.	
BB:CategoryDefinition: Session Closed	Category Definition	Event	Edit this BB to define all session closed events.	
BB:CategoryDefinition: Session Opened	Category Definition	Event	Edit this BB to define all session opened events.	
BB:CategoryDefinition: Suspicious Event Categories	Category Definitions	Event	Edit this BB to include all event categories that indicate suspicious activity.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Suspicious Events	Category Definitions	Common	Edit this BB to include all events that indicate suspicious activity.	
BB:CategoryDefinition: System Configuration	Category Definitions	Event	Edits this BB to define system configuration events.	
BB:CategoryDefinition: System Errors and Failures	Category Definitions	Event	Edit this BB to define system errors and failures.	
BB:CategoryDefinition: Upload to Local WebServer	Category Definitions	Event	Typically, most networks are configured to restrict applications that use the PUT method running on their web application servers. This BB detects if a remote host has used this method on a local server. The BB can be duplicated to also detect other unwanted methods or for local hosts using the method connecting to remote servers. This BB is referred to by the Policy: Upload to Local WebServer rule.	
BB:CategoryDefinition: Virus Detected	Category Definition	Event	Edit this BB to define all virus detection events.	
BB:CategoryDefinition: VoIP Authentication Failure Events	Category Definitions	Event	Edit this BB to include all events that indicate a VoIP login failure.	
BB:CategoryDefinition: VoIP Session Opened	Category Definitions	Event	Edit this BB to include all events that indicate the start of a VoIP session.	
BB:CategoryDefinition: VPN Access Accepted	Category Definition	Event	Edit this BB to include all events that indicates permitted access.	
BB:CategoryDefinition: VPN Access Denied	Category Definition	Event	Edit this BB to include all events that are considered Denied Access events.	
BB:CategoryDefinition: Windows Compliance Events	Compliance	Event	Edit this BB to include all event categories that indicate compliance events.	
BB:CategoryDefinition: Windows SOX Compliance Events	Compliance	Event	Edit this BB to include all event categories that indicate SOX compliance events.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:CategoryDefinition: Worm Events	Category Definitions	Event	Edit this BB to define worm events. This BB only applies to events not detected by a custom rule.	
BB:ComplianceDefinition: GLBA Servers	Compliance	Common	Edit this BB to include your GLBA IP systems. You must then apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: HIPAA Servers	Compliance	Common	Edit this BB to include your HIPAA Servers by IP address. You must then apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: PCI DSS Servers	Response	Common	Edit this BB to include your PCI DSS servers by IP address. You must apply this BB to rules related to failed logins such as remote access.	
BB:ComplianceDefinition: SOX Servers	Compliance	Common	Edit this BB to include your SOX IP Servers. You must then apply this BB to rules related to failed logins such as remote access.	
BB:Database: System Action Allow	Compliance	Event	Edit this BB to include any events that indicates successful actions within a database.	
BB:Database: System Action Deny	Compliance	Event	Edit this BB to include any events that indicate unsuccessful actions within a database.	
BB:Database: User Addition or Change	Compliance	Event	Edit this BB to include events that indicate the successful addition or change of user privileges	
BB:DeviceDefinition: Access/Authentication/ Audit	Log Source Definitions	Event	Edit this BB to include all access, authentication, and audit devices.	
BB:DeviceDefinition: AntiVirus	Log Source Definitions	Event	Edit this BB to include all antivirus services on the system.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:DeviceDefinition: Application	Log Source Definitions	Event	Edit this BB to include all application and OS devices on the network.	
BB:DeviceDefinition: Consumer Grade Routers	Log Source Definitions	Event	Edit this BB to include MAC addresses of known consumer grade routers.	
BB:DeviceDefinition: Consumer Grade Wireless APs	Log Source Definitions	Event	Edit this BB to include MAC addresses of known consumer grade wireless access points.	
BB:DeviceDefinition: Database	Log Source Definitions	Event	Edit this BB to define all databases on the system.	
BB:DeviceDefinition: Devices to Monitor for High Event Rates	Log Source Definitions	Event	Edit this BB to include devices you want to monitor for high event rates. The event rate threshold is controlled by the Anomaly: Devices with High Event Rates.	
BB:DeviceDefinition: FW/Router/ Switch	Log Source Definitions	Event	Edit this BB to include all firewall (FW), routers, and switches on the network.	
BB:DeviceDefinition: IDS/IPS	Log Source Definitions	Event	Edit this BB to include all IDS and IPS devices on the network.	
BB:DeviceDefinition:VPN	Log Source Definition	Event	Edit this BB to include all VPNs on the network.	
BB:FalseNegative: Events That Indicate Successful Compromise	False Positive	Event	Edit this BB to include events that indicate a successful compromise. These events generally have 100% accuracy.	
BB:FalsePositive: All Default False Positive BBs	False Positive	Common	Edit this BB to include all false positive BBs.	All BB:False Positive BBs
BB:FalsePositive: Broadcast Address False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from the broadcast address space.	
BB:FalsePositive: Database Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from database servers that are defined in the BB:HostDefinition: Database Servers BB.	BB:HostDefinition: Database Servers

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:FalsePositive: Database Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from database servers that are defined in the BB:HostDefinition: Database Servers BB.	BB:HostDefinition: Database Servers
BB:FalsePositive: Device and Specific Event	False Positive	Event	Edit this BB to include the devices and QID of devices that continually generate false positives.	
BB:FalsePositive: DHCP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from DHCP servers that are defined in the BB:HostDefinition: DHCP Servers BB.	BB:HostDefinition: DHCP Servers
BB:FalsePositive: DHCP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DHCP servers that are defined in the BB:HostDefinition: DHCP Servers BB.	BB:HostDefinition: DHCP Servers
BB:FalsePositive: DNS Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from DNS based servers that are defined in the BB:HostDefinition: DNS Servers BB.	BB:HostDefinition: DNS Servers
BB:FalsePositive: DNS Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DNS-based servers that are defined in the BB:HostDefinition: DNS Servers BB.	BB:HostDefinition: DNS Servers
BB:FalsePositive: Firewall Deny False Positive Events	False Positive	Event	Edit this BB to define firewall deny events that are false positives	
BB:FalsePositive: FTP False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from FTP-based servers that are defined in the BB:HostDefinition: FTP Servers BB.	BB:HostDefinition: FTP Servers

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:FalsePositive: FTP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from FTP based servers that are defined in the BB:HostDefinition: FTP Servers BB.	BB:HostDefinition: FTP Servers
BB:FalsePositive: Global False Positive Events	False Positive	Event	Edit this BB to include any event QIDs that you want to ignore.	
BB:FalsePositive: Large Volume Local FW Events	False Positive	Event	Edit this BB to define specific events that can create a large volume of false positives in general rules.	
BB:FalsePositive: LDAP Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from LDAP servers that are defined in the BB:HostDefinition: LDAP Servers BB.	BB:HostDefinition: LDAP Servers
BB:FalsePositive: LDAP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from LDAP servers that are defined in the BB:HostDefinition: LDAP Servers BB.	BB:HostDefinition: LDAP Servers
BB:FalsePositive: Local Source to Local Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Local (L2L) based servers.	
BB:FalsePositive: Local Source to Remote Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Remote (L2R) based servers.	
BB:FalsePositive: Mail Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from mail servers that are defined in the BB:HostDefinition: Mail Servers BB.	BB:HostDefinition: Mail Servers
BB:FalsePositive: Mail Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from mail servers that are defined in the BB:HostDefinition: Mail Servers BB.	BB:HostDefinition: Mail Servers

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:FalsePositive: Network Management Servers Recon	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from network management servers that are defined in the BB:HostDefinition: Network Management Servers BB.	BB:HostDefinition: Network Management Servers
BB:FalsePositive: Proxy Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from proxy servers that are defined in the BB:HostDefinition: Proxy Servers BB.	BB:HostDefinition: Proxy Servers
BB:FalsePositive: Proxy Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from proxy servers that are defined in the BB:HostDefinition: Proxy Servers BB.	BB:HostDefinition: Proxy Servers
BB:FalsePositive: Remote Source to Local Destination False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Remote-to-Local (R2L) based servers.	
BB:FalsePositive: RPC Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from RPC servers that are defined in the BB:HostDefinition: RPC Servers BB.	BB:HostDefinition: RPC Servers
BB:FalsePositive: RPC Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from RPC servers that are defined in the BB:HostDefinition: RPC Servers BB.	BB:HostDefinition: RPC Servers
BB:FalsePositive: SNMP Sender or Receiver False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from SNMP servers that are defined in the BB:HostDefinition: SNMP Servers BB.	BB:HostDefinition: SNMP Servers

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:FalsePositive: SNMP Sender or Receiver False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SNMP servers that are defined in the BB:HostDefinition: SNMP Sender or Receiver BB.	BB:HostDefinition: SNMP Sender or Receiver
BB:FalsePositive: Source IP and Specific Event	False Positive	Event	Edit this BB to include source IP addresses or specific events that you want to remove.	
BB:FalsePositive: SSH Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from SSH servers that are defined in the BB:HostDefinition: SSH Servers BB.	BB:HostDefinition: SSH Servers
BB:FalsePositive: SSH Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SSH servers that are defined in the BB:HostDefinition: SSH Servers BB.	BB:HostDefinition: SSH Servers
BB:FalsePositive: Syslog Sender False Positive Categories	False Positive	Common	Edit this BB to define all false positive categories that occur to or from syslog sources.	BB:HostDefinition: Syslog Servers and Senders
BB:FalsePositive: Syslog Sender False Positive Events	False Positive	Event	Edit this BB to define all false positive events that occur to or from syslog sources or destinations.	BB:HostDefinitionBB:HostDefinition: Syslog Servers and Senders
BB:FalsePositive: Virus Definition Update Categories	False Positive	Common	Edit this BB to define all the false positive QIDs that occur to or from virus definition or other automatic update hosts that are defined in the BB:HostDefinition: Virus Definition and Other Update Servers BB.	BB:HostDefinition: Virus Definition and Other Update Servers
BB:FalsePositive: Web Server False Positive Categories	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from web servers that are defined in the BB:HostDefinition: Web Servers BB.	BB:HostDefinition: Web Servers

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:FalsePositive: Web Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Web servers that are defined in the BB:HostDefinition: Web Servers BB.	BB:HostDefinition: Web Servers
BB:FalsePositive: Windows AD Source Authentication Events	False Positive	Event	Edit this BB to add addresses of Windows Authentication and Active Directory (AD) servers. This BB prevents the AD servers from being the source of authentication messages.	
BB:FalsePositive: Windows Server False Positive Categories Local	False Positive	Common	Edit this BB to define all the false positive categories that occur to or from Windows servers that are defined in the BB:HostDefinition: Windows Servers BB.	BB:HostDefinition: Windows Servers
BB:FalsePositive: Windows Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Windows servers that are defined in the BB:HostDefinition: Windows Servers BB.	BB:HostDefinition: Windows Servers
BB:NetworkDefinition: Broadcast Address Space	Network Definition	Common	Edit this BB to include the broadcast address space of your network. This is used to remove false positive events that might be caused by the use of broadcast messages.	
BB:NetworkDefinition: Client Networks	Network Definition	Common	Edit this BB to include all networks that include client hosts.	
BB:NetworkDefinition: Darknet Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Darket list.	
BB:NetworkDefinition: DLP Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Data Loss Prevention (DLP) list.	
BB:NetworkDefinition: DMZ Addresses	Network Definition	Common	Edit this BB to include networks that you want to add to a Demilitarized Zone (DMZ) list.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:NetworkDefinition: DMZ Addresses(DST)	Network Definition	Common	Edit this BB to include destination networks that you want to add to a Demilitarized Zone (DMZ) list.	
BB:NetworkDefinition: DMZ Addresses(SRC)	Network Definition	Common	Edit this BB to include source networks that you want to add to a Demilitarized Zone (DMZ) list.	
BB:NetworkDefinition: Honeypot like Addresses	Network Definition	Common	Edit this BB by replacing other network with network objects defined in your network hierarchy that are currently not in use in your network or are used in a honeypot or tarpit installation. When these have been defined, you must enable the Anomaly: Potential Honeypot Access rule. You must also add a security or policy BB to these network objects to generate events based on attempted access.	
BB:NetworkDefinition: Inbound Communication from Internet to Local Host	Network Definition	Common	Edit this BB to include all traffic from the Internet to you local networks.	
BB:NetworkDefinition: Multicast Address Space	Network Definition	Common	Edit this BB to include networks that you want to add to a multicast address space list.	
BB:NetworkDefinition: NAT Address Range	Network Definition	Common	Edit this BB to define typical Network Address Translation (NAT) range you want to use in your deployment.	
BB:NetworkDefinition: Server Networks	Network Definition	Common	Edit this BB to include the networks where your servers are located.	
BB:NetworkDefinition: Trusted Network Segment	Network Definition	Common	Edit this BB to include event categories that are trusted local networks.	
BB:NetworkDefinition: Undefined IP Space	Network Definition	Common	Edit this BB to include areas of your network that does not contain any valid hosts.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:NetworkDefinition: Untrusted Local Networks	Network Definition	Common	Edit this BB to include untrusted local networks.	
BB:NetworkDefinition: Untrusted Network Segment	Network Definition	Common	Edit this BB to include any untrusted networks.	BB:NetworkDefinition: Untrusted Local Network BB:NetworkDefinition: Inbound Communication from Internet to Local Host
BB:NetworkDefinition: Watch List Addresses	Network Definition	Common	Edit this BB to include networks that should be added to a watch list.	
BB:Policy: Application Policy Violation Events	Policy	Event	Edit this BB to define policy application and violation events.	
BB:Policy: IRC/IM Connection Violations	Policy	Event	Edit this BB to define all policy IRC and IM connection violations.	
BB:Policy: Policy P2P	Policy	Event	Edit this BB to include all events that indicate P2P events.	
BB:PortDefinition: Authorized L2R Ports	Port\ Protocol Definition	Common	Edit this BB to include ports that are commonly detected in Local-to-Remote (L2R) traffic.	
BB:PortDefinition: Common Worm Ports	Port\ Protocol Definition	Common	Edit this BB to include all ports that are generally not seen in L2R traffic.	
BB:PortDefinition: Database Ports	Port\ Protocol Definition	Common	Edit this BB to include all common database ports.	
BB:PortDefinition: DHCP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common DHCP ports.	
BB:PortDefinition: DNS Ports	Port\ Protocol Definition	Common	Edit this BB to include all common DNS ports.	
BB:PortDefinition: FTP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common FTP ports.	
BB:PortDefinition: Game Server Ports	Port\ Protocol Definition	Common	Edit this BB to include all common game server ports.	
BB:PortDefinition: IM Ports	Compliance	Common	Edit this BB to include all common IM ports.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:PortDefinition: IRC Ports	Port\ Protocol Definition	Common	Edit this BB to include all common IRC ports.	
BB:PortDefinition: LDAP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by LDAP servers.	
BB:PortDefinition: Mail Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by mail servers.	
BB:PortDefinition: P2P Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by P2P servers.	
BB:PortDefinition: Proxy Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by proxy servers.	
BB:PortDefinition: RPC Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by RPC servers.	
BB:PortDefinition: SNMP Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by SNMP servers.	
BB:PortDefinition: SSH Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by SSH servers.	
BB:PortDefinition: Syslog Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by the syslog servers.	
BB:PortDefinition: Web Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by Web servers.	
BB:PortDefinition: Windows Ports	Port\ Protocol Definition	Common	Edit this BB to include all common ports used by Windows servers.	
BB:ProtocolDefinition: Windows Protocols	Port\ Protocol Definition	Common	Edit this BB to include all common protocols (not including TCP) used by Windows servers that will be ignored for false positive tuning rules.	

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
BB:Recon Detected: All Recon Rules	Recon	Event	Edit this BB to define all IBM default reconnaissance tests. This BB is used to detect a host that has performed reconnaissance such that other follow on tests can be performed. For example, reconnaissance followed by firewall accept.	
BB:Recon Detected: Host Port Scan	Recon	Event	Edit this BB to define reconnaissance scans on hosts in your deployment.	
BB:Recon Detected: Port Scan Detected Across Multiple Hosts	Recon	Event	Edit this BB to indicate port scanning activity across multiple hosts. By default, this BB applies when a source IP address is performing reconnaissance against more than five hosts within 10 minutes. If internal, this might indicate an exploited system or a worm scanning for destination IP addresses.	
User-BB:FalsePositive: User Defined False Positives Tunings	User Tuning	Common	This BB contains any events that you have tuned using the False Positive tuning function. For more information, see the *IBM Security QRadar Log Manager Users Guide*.	
User-BB:FalsePositive: Server Type 1 - User Defined False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User-BB:HostDefinition: Server Type 1 - User Defined
User-BB:FalsePositive: Server Type 1 - User Defined False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined in the associated BB.	User-BB:HostDefinition: Server Type 1 - User Defined
User-BB:FalsePositive: User Defined Server Type 2 False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 2 - User Defined

Table 10-2 Default building blocks (continued)

Building block	Group	Block type	Description	Associated building blocks, if applicable
User-BB:FalsePositive: User Defined Server Type 2 False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 2 - User Defined
User-BB:FalsePositive: User Defined Server Type 3 False Positive Categories	User Tuning	Event	Edit this BB to include any event categories you want to consider false positives for hosts defined in the associated BB.	User:BB:HostDefinition: Server Type 3 - User Defined
User-BB:FalsePositive: User Defined Server Type 3 False Positive Events	User Tuning	Event	Edit this BB to include any events you want to consider false positives for hosts defined the associated BB.	User:BB:HostDefinition: Server Type 3 - User Defined
User-BB:HostDefinition: Server Type 1 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the associated BBs.	User-BB:FalsePositives: Server Type 1 - User Defined False Positive Category User-BB:False Positives: Server Type 1 - User Defined False Positive Events
User-BB:HostDefinition: Server Type 2 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the associated BBs.	User-BB:FalsePositives: User Defined Server Type 2 False Positive Category User-BB:False Positives: User Defined Server Type 2 False Positive Events
User-BB:HostDefinition: Server Type 3 - User Defined	User Tuning	Event	Edit this BB to include the IP address of your custom server type. After you have added the servers, add any events or event categories you want to consider false positives to these servers as defined in the as defined in the associated BBs.	User-BB:FalsePositives: User Defined Server Type 3 False Positive Category User-BB:False Positives: User Defined Server Type 3 False Positive Events

B GLOSSARY

active system In a High Availability (HA) cluster, the active system is the system with all services running. Either the primary or secondary HA host can be the active host. If the secondary HA host is the active host, failover has occurred.

accumulator The accumulator resides on the host that contains an Event Processor to assist with analyzing events, reporting, writing database data, and alerting a DSM.

Address Resolution Protocol (ARP) A protocol for mapping an Internet Protocol (IP) address to a physical host address recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet LAN, however, addresses for attached devices are 48 bits long.

anomaly A deviation from expected behavior of the network.

application signature A unique set of characteristics or properties, derived by the examination of packet payload, used to identify a specific application.

ARP See Address Resolution Protocol.

ARP Redirect ARP allows a host to determine the address of other devices on the LAN or VLAN. A host can use ARP to identify the default gateway (router) or path off to the VLAN. ARP Redirect allows QRadar Log Manager to notify a host if a problem exists with sending traffic to a system. This renders the host and network unusable until the user intervenes.

ASN See Autonomous System Number.

Autonomous System Number An autonomous system is a collection of IP networks that all adhere to the same specific and clearly defined routing policy. An Autonomous System Number (ASN) is a unique ID number assigned to each autonomous system.

behavior Indicates the normal manner in which the system or network functions or operates.

branding A reporting option that enables a QRadar Log Manager user to upload custom logos for customized reports.

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
Addressing scheme for the Internet, which allocates and species Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.

client
The host that originates communication.

Cluster Virtual IP address
The Cluster Virtual IP address is the IP address used to communicate with an HA cluster. When you configure HA, the IP address of the primary HA host becomes the Cluster Virtual IP address. If the primary HA host fails, the Cluster Virtual IP address will be assumed by the secondary HA host.

coalescing interval
The interval for coalescing (bundling) events is 10 seconds, beginning with the first event that does not match any currently coalescing events. Within the interval, the first three matching events are released immediately to the Event Processor and the fourth and subsequent events are coalesced such that the payload and other features are kept from the fourth event. Each arrival of a matching event during the interval increments the event count of the fourth event. At the end of the interval, the coalesced event is released to the Event Processor and the next interval begins for matching events. If no matching events arrive during this interval, the process restarts. Otherwise, the coalescing continues with all events counted and released in 10 second intervals.

Console
Web interface for QRadar Log Manager. QRadar Log Manager is accessed from a standard web browser (Internet Explorer 7.0/8.0 or Mozilla Firefox 3.6 and above). When you access the system, a prompt is displayed for a user name and password, which must be configured in advance by the QRadar Log Manager administrator.

credibility
Indicates the integrity of an event as determined by the credibility rating that is configured in the log source. Credibility increases as the multiple sources report the same event.

database leaf objects
The end point objects in a hierarchy. At each point in the hierarchy above this point there is a parent object that contains the aggregate values of all of the leaf objects below.

datapoint
Any point on the QRadar Log Manager charts where data is extracted.

DHCP
See Dynamic Host Configuration Protocol.

Device Support Module (DSM)
Device Support Modules (DSMs) allows you to integrate QRadar Log Manager with log sources.

DNS
See Domain Name System.

DSM
See Device Support Module (DSM).

Domain Name System (DNS)
An online, distributed database used to map human-readable machine names into an IP address for resolving machine names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)
A protocol that allows dynamic assignment of IP addresses to customer premise equipment.

encryption
Encryption provides greater security for all QRadar Log Manager traffic between managed hosts. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host to provide protected access to the servers.

event
Record from a device that describes an action on a network or host.

Event Collector
Collects security events from various types of devices in your network. The Event Collector gathers eventsfrom local, remote, and device sources. The Event Collector then normalizes the events, and sends the information to the Event Processor.

Event Processor
Processes events collected from one or more Event Collectors. The events are bundled once again to conserve network usage. When received, the Event Processor correlates the information from QRadar Log Manager and distributed to the appropriate area, depending on the type of event.

forwarding destination
QRadar Log Manager allows you to forward raw log data received from log sources and QRadar Log Manager-normalized event data to one or more vendor systems, such as ticketing or alerting systems. On the QRadar Log Manager user interface, these vendor systems are called forwarding destinations.

Fully Qualified Domain Name (FQDN)
The portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to.

Fully Qualified Network Name (FQNN)
Full path name of a certain point in the network hierarchy. For example, Company A hierarchy has a department object that contains a marketing object. Therefore, the FQNN is CompanyA.Department.Marketing.

FQDN
See Fully Qualified Domain Name.

FQNN
See Fully Qualified Network Name.

gateway
A device that communicates with two protocols and translates services between them.

HA
See High Availability.

HA cluster
An HA cluster consists of a primary HA host and a secondary HA host that behaves as a standby for the primary.

Hash-Based Message Authentication Code (HMAC) A cryptographic code that uses a cryptic hash function and a secret key.

High Availability The High Availability (HA) feature ensures availability of QRadar Log Manager data in the event of a hardware or network failure. An HA cluster consists of a primary host and a secondary host that acts as a standby for the primary. The secondary host maintains the same data as the primary host by one of two methods: data replication or shared external storage. At regular intervals, every 10 seconds by default, the secondary host sends a heartbeat ping to the primary host to detect hardware and network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host.

HMAC See Hash-based Message Authentication Code (HMAC).

Host Context Monitors all QRadar Log Manager components to ensure that each component is operating as expected.

ICMP See Internet Control Message Protocol.

identity QRadar Log Manager collects identity information, if available, from log source messages. Identity information provides additional details about assets on your network. Log sources only generate identity information if the log message sent to QRadar Log Manager contains an IP address and at least one of the following items: user name or MAC address. Not all log sources generate identity information.

IDS See Intrusion Detection System.

Internet Control Message Protocol (ICMP) An Internet network-layer protocol between a host and gateway.

Internet Protocol (IP) The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.

Internet Service Provider (ISP) An Internet Service Provider (ISP) provides users access to the Internet and other related services.

Intrusion Detection System (IDS) An application or device that identifies suspicious activity on the network.

Intrusion Prevention System (IPS) Application that reacts to network intrusions.

IP See Internet Protocol.

IP Multicast IP Multicast reduces traffic on a network by delivering a single stream of information to multiple users at one time.

IP network A group of IP routers that route IP datagrams. These routers are sometimes referred to as Internet gateways. Users access the IP network from a host. Each network in the Internet includes some combination of hosts and IP routers.

IPS See Intrusion Prevention System.

item A Dashboard option that creates a customized portal that displays any permissible view for monitoring purposes.

L2L See Local To Local.

L2R See Local To Remote.

LAN See Local Area Network.

LDAP See Lightweight Directory Access Protocol.

leaves Children or objects which are part of a parent group.

Lightweight Directory Access Protocol (LDAP) A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access to a directory server.

Local Area Network (LAN) A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Local To Local (L2L) Internal traffic from one local network to another local network.

Local To Remote (L2R) Internal traffic from a local network to a remote network.

log source Log sources are external event log sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers).

Magistrate Provides the core processing components of the SIEM option. The Magistrate provides reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules.

NAT See Network Address Translation (NAT).

Network Address Translation (NAT) NAT translates an IP address in one network to a different IP address in another network.

network hierarchy Contains each component of your network, and identifies which objects belong within other objects. The accuracy and completeness of this hierarchy is essential to traffic analysis functions. The network hierarchy provides for storage of logs, databases, and TopN files.

network layer Layer 3 in the Open System Interconnection (OSI) architecture; the layer that establishes a path between open systems.

network objects Components of your network hierarchy. You can add layers to the hierarchy by adding additional network objects and associating them to already defined objects. (Objects that contain other objects are called groups.)

network weight The numeric value applied to each network that signifies the importance of the network. The network weight is user defined.

Off-site source An off-site device that forwards normalized data to an Event Collector. You can configure an off-site source to receive events and allow the data to be encrypted before forwarding.

Off-site Target An off-site device that receives event data. An off-site target can only receive data from an Event Collector.

Open Systems Interconnection (OSI) A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

OSI See Open Systems Interconnection.

primary HA host In an HA cluster, the primary HA host is the host to which you want to add HA protection. You can configure HA for any system (Console or non-Console) in your deployment. When you configure HA, the IP address of the primary HA host becomes the Cluster Virtual IP address; therefore, you must configure a new IP address for the primary host.

protocol A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It might still require an authorization exchange with a policy module or external policy server before admission.

QID QRadar Log Manager Identifier. A mapping of a single event of an external device to a IBM unique identifier.

R2L See Remote To Local.

R2R See Remote To Remote.

refresh timer The **Dashboard**, **Log Activity**, and **Network Activity** tabs feature a dynamic status bar that displays the amount of time until QRadar Log Manager automatically refreshes the current network activity data; built-in refresh can be manually refreshed at any time.

relevance Relevance determines the impact on your network of an event or category. For example, if a certain port is open, the relevance is high.

Remote To Local (R2L) External traffic from a remote network to a local network.

Remote To Remote (R2R) External traffic from a remote network to another remote network.

reports A function that creates executive or operational level charting representations of network activity based on time, sources, security, and events.

report interval A configurable time interval at which the Event Processor must send all captured event data to the Console.

routing rules Collection of conditions and consequent routing that are performed when event data matches each rule.

rule Collection of conditions and consequent actions. You can configure rules that allow QRadar Log Manager to capture and respond to specific event sequences. The rules allow you to detect specific, specialized events and forward notifications to either the log file, or email a user.

secondary HA host In an HA cluster, the secondary HA host is the standby for the primary host. If the primary HA host fails, the secondary HA host automatically assumes all responsibilities of the primary HA host.

severity Indicates the amount of threat a source poses in relation to how prepared the destination is for the attack. This value is mapped to an event category in the QID map that is correlated to the event.

Simple Network Management Protocol (SNMP) A network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.

Simple Object Access Protocol (SOAP) A protocol that allows a program running in one kind of operating system to communicate with a program in the same or another kind of an operating system.

SNMP See Simple Network Management Protocol.

SOAP See Simple Object Access Protocol.

standby system In an HA cluster, the standby system is the host that is acting as standby for the active system. Only the secondary HA host can be the standby system. The standby system has no services running. If disk replication is enabled, the standby system is replicating data from the active system. If the active system fails, the standby system automatically assumes the active role.

subnet A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.

subnet mask A bit mask that is logically ANDed with the destination IP address of an IP packet to determine the network address. A router routes packets using the network address.

sub-search Allows you to perform searches within a set of completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again.

System Time The right corner of the user interface displays System time, which is the time on the QRadar Log Manager Console. This is the time that determines the time of events.

System View Allows you to assign software components to systems (managed hosts) in your deployment. The System View includes all managed hosts in your deployment. A managed host is a system in your deployment that has QRadar Log Manager software installed.

TACACS Terminal Access Controller Access Control System (TACACS) is an authentication protocol that allows remote server access to forward a user logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ uses TCP.

TCP See Transmission Control Protocol.

TCP flags A type of marker that can be added to a packet to alert the system of abnormal activity. Only a few specific combinations of flags are valid and typical, in normal traffic. Abnormal combinations of flags often indicate an attack or an abnormal network condition.

TCP resets For TCP-based applications, QRadar Log Manager can issue a TCP reset to either the client or server in a conversation. This stops the communications between the client and the server.

Time Series A chart type that graphs data based on time. This chart focuses on the networks or IP address data information from the selected networks.

TopN Displays the top *N* networks or IP address information for the data you are viewing. For example, using the chart feature, you can display the top five networks generating traffic in the U.S.

Transmission Control Protocol (TCP) A reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.

violation Includes a violation of corporate policy.

Whois Allows you to look up information about registered Internet names and numbers.

C NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

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

IBM might 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 might be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right might 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 might 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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might 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 might make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

Licensees of this program who want 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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information might 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.

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

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices might 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Trademarks

IBM, the IBM logo, and 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 *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

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

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

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

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

INDEX