IBM Security QRadar Log Manager
Version 7.2.2

Users Guide
Before using this information and the product that it supports, read the information in “Notices” on page 141.
Contents

About the QRadar Log Manager Users Guide ........................................ vii

Chapter 1. What's new for users in QRadar Log Manager V7.2.2 .............. 1

Chapter 2. About QRadar Log Manager ................................................. 3
Supported web browsers ........................................................................ 3
Enabling document mode and browser mode in Internet Explorer .......... 3
Access IBM Security QRadar ............................................................... 4
User interface tabs ............................................................................. 4
  Dashboard tab .................................................................................. 4
  Log activity tab .................................................................................. 4
  Assets tab .......................................................................................... 4
  Reports tab ......................................................................................... 5
  IBM Security QRadar Vulnerability Manager tab ......................... 5
Admin tab ............................................................................................ 5
QRadar common procedures ............................................................... 6
Viewing messages ............................................................................... 6
Sorting results .................................................................................... 8
Refreshing and pausing the user interface ......................................... 8
Investigating IP addresses ................................................................. 9
Investigate user names ...................................................................... 10
System time .......................................................................................... 11
Updating user preferences .................................................................. 11
Access online help ........................................................................... 12
Resize columns ................................................................................... 12
Configure page size ........................................................................... 12

Chapter 3. Dashboard management ..................................................... 13
Log activity .......................................................................................... 13
Most recent reports ........................................................................... 15
System summary ................................................................................ 15
Vulnerability Management items ....................................................... 15
System notification ............................................................................ 15
Adding dashboard items .................................................................... 16
Using the dashboard to investigate log activity ................................ 16
Configuring charts ............................................................................. 17
Removing dashboard items ............................................................... 18
Detaching a dashboard item .............................................................. 19
Renaming a dashboard ..................................................................... 19
Deleting a dashboard ........................................................................ 19
Managing system notifications .......................................................... 20
Adding search-based dashboard items to the Add Items list ............. 20

Chapter 4. Log activity investigation ................................................... 23
Log activity tab overview ................................................................. 23
  Log activity tab toolbar ................................................................... 23
  Quick filter syntax .......................................................................... 27
  Right-click menu options ............................................................. 27
  Status bar ......................................................................................... 28
Log activity monitoring ...................................................................... 28
  Viewing streaming events .............................................................. 28
  Viewing normalized events .......................................................... 29
  Viewing raw events ....................................................................... 31
  Viewing grouped events ............................................................... 33

© Copyright IBM Corp. 2012, 2013

iii
Event details .................................. 38
Event details toolbar ............................... 41
Modifying event mapping .............................. 42
Managing PCAP data .................................. 43
  Displaying the PCAP data column. .................. 43
  Viewing PCAP information ........................... 44
  Downloading the PCAP file to your desktop system. .. 45
Exporting events .................................. 45

Chapter 5. Chart management. ......................... 47
  Time series chart overview .......................... 47
  Chart legends ................................ 49
  Configuring charts ................................ 49

Chapter 6. Data searches. .............................. 51
  Searching for items that match your criteria ........ 51
  Saving search criteria ................................ 56
  Deleting search criteria ............................. 57
  Using a subsearch to refine search results .......... 58
  Managing search results ................................ 59
    Saving search results ................................ 59
    Viewing managed search results ................. 59
    Canceling a search .................................. 61
    Deleting a search ................................ 61
  Managing search groups ................................ 62
    Viewing search groups ............................ 62
    Creating a new search group ...................... 63
    Editing a search group ............................. 63
    Copying a saved search to another group ......... 63
    Removing a group or a saved search from a group .. 64

Chapter 7. Custom event properties ...................... 65
  Required permissions ................................ 65
  Custom property types ................................ 65
  Creating a regex-based custom property ............. 66
  Creating a calculation-based custom property ......... 67
  Modifying a custom property .......................... 69
  Copying a custom property ......................... 71
  Deleting a custom property ......................... 71

Chapter 8. Rule management .............................. 73
  Rule permission considerations ....................... 73
  Rules overview ................................ 73
    Event rule ................................ 73
    Rule conditions ................................ 73
    Rule responses ................................ 74
  Viewing rules ................................ 75
  Creating a custom rule ................................ 75
  Creating an anomaly detection rule ................... 76
  Rule management tasks ................................ 78
    Enabling and disabling rules ....................... 78
    Editing a rule ................................ 78
    Copying a rule ................................ 79
    Deleting a rule ................................ 79
  Rule group management ................................ 80
    Viewing a rule group .............................. 80
    Creating a group ................................ 80
    Assigning an item to a group .................... 80
    Editing a group ................................ 81
    Copying an item to another group ................ 81
About the QRadar Log Manager Users Guide

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

Intended audience

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

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

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

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.
Chapter 1. What's new for users in QRadar Log Manager V7.2.2

IBM Security QRadar Log Manager V7.2.2 introduces updates to user preferences for language selection, select different locales for numeric values, view system messages, and interface with user supplied data.

**Users can set their language preference**

QRadar is available in the following languages: English, Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, Italian, Spanish, and Portuguese (Brazil). Users can select their preferred language by using choosing the Locale setting in the Preferences list. [Learn more...](#)

**Support numeric values in different locales for custom events**

QRadar now has the ability to support numeric values using different locales for custom events. [Learn more...](#)

**New user roles can view system notifications**

Users can see system notifications on the Dashboard.

**New user roles can interface with their data**

Users can interface with collections of data that they supply.
Chapter 2. 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.

**Navigate the web-based application**

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

**Supported web browsers**

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Supported version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>17.0 Extended Support Release</td>
</tr>
<tr>
<td></td>
<td>24.0 Extended Support Release</td>
</tr>
<tr>
<td>32-bit Microsoft Internet Explorer, with document mode and browser mode enabled</td>
<td>8.0</td>
</tr>
<tr>
<td></td>
<td>9.0</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>The current version as of the release date of IBM Security QRadar V7.2.2 products</td>
</tr>
</tbody>
</table>

**Enabling document mode and browser mode in Internet Explorer**

If you use Microsoft Internet Explorer to access IBM Security QRadar products, you must enable browser mode and document mode.

**Procedure**

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode**.
   - For Internet Explorer V9.0, select **Internet Explorer 9 standards**
   - For Internet Explorer V8.0, select **Internet Explorer 8 standards**
**Access IBM Security QRadar**

IBM Security QRadar is a web-based application. QRadar uses default login information for the URL, user name, and password.

Use the information in the following table when you log in to your IBM Security QRadar console.

*Table 2. Default login information for QRadar*

<table>
<thead>
<tr>
<th>Login information</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>https://&lt;IP Address&gt;, where &lt;IP Address&gt; is the IP address of the QRadar console. To log in to QRadar in an IPv6 or mixed environment, wrap the IP address in square brackets: https://[&lt;IP Address&gt;]</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is assigned to QRadar during the installation process.</td>
</tr>
<tr>
<td>License key</td>
<td>A default license key provides you access to the system for 5 weeks.</td>
</tr>
</tbody>
</table>

**User interface tabs**

Functionality is divided into tabs. The **Dashboard** tab is displayed when you log in.

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.

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

**Log activity tab**

The **Log Activity** tab will allow you to investigate event logs being sent to QRadar in real-time, perform powerful searches, and view log activity by using configurable time-series charts.

The **Log Activity** tab will allow you to perform in-depth investigations on event data.

For more information, see [Log Activity investigation](#)

**Assets tab**

QRadar automatically discovers assets, servers, and hosts, operating on your network.

---

4 QRadar Log Manager Users Guide
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, an attack tries to use a specific service that is running on a specific asset. In this situation, QRadar can determine whether 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.

**Reports tab**

The Reports tab will allow you to create, distribute, and manage reports for any data within QRadar.

The Reports feature will allow 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 preinstalled report templates that are included with QRadar.

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

For more information about reports, see Reports management.

**IBM Security QRadar Vulnerability Manager tab**

IBM Security QRadar Vulnerability Manager is a QRadar component that you can purchase separately. You use a license key to enable QRadar Vulnerability Manager.

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 rerun scans to evaluate the new level of risk.

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

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

**Admin tab**

Administrators use the Admin tab to configure and manage the users, systems, networks, plug-ins, and components. Users with administration privileges can access the Admin tab.

The administration tools that administrators can access in the Admin tab are described in Table 1.
Table 3. Administration management tools available in QRadar

<table>
<thead>
<tr>
<th>Admin tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>Configure system and user management options.</td>
</tr>
<tr>
<td>Data Sources</td>
<td>Configure log sources.</td>
</tr>
<tr>
<td>Remote Networks and Services Configuration</td>
<td>Configure remote networks and services groups.</td>
</tr>
<tr>
<td>Plug-ins</td>
<td>Access plug-in components, such as the IBM Security QRadar Risk Manager plug-in. This option is only displayed if there are plug-ins that are installed on your Console.</td>
</tr>
<tr>
<td>Deployment Editor</td>
<td>Manage the individual components of your QRadar deployment.</td>
</tr>
</tbody>
</table>

All configuration updates that 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.

**QRadar common procedures**

Various controls on the QRadar user interface are common to most user interface tabs.

Information about these common procedures is described in the following sections.

**Viewing messages**

The Messages menu, which is on the upper 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 that is based on each notification message type and select the Notify check box in the Custom Rules Wizard.

**About this task**

The Messages menu indicates how many unread system notifications you have in your system. This indicator increments the number until you close 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 close a system notification from the Messages window, the system notification is removed from all system notification displays.
The **Messages** window provides the following functions:

**Table 4. Functions available in the Messages window**

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

### Procedure

1. Log in to QRadar.
2. On the upper right corner of the user interface, click **Messages**.
3. On the Messages window, view the system notification details.
4. Optional. To refine the list of system notifications, click one of the following options:
   - Errors
   - Warnings
   - Information
5. Optional. To close system notifications, choose one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismiss All</td>
<td>Click to close all system notifications.</td>
</tr>
<tr>
<td>Dismiss</td>
<td>Click the Dismiss icon next to the system notification that you want to close.</td>
</tr>
</tbody>
</table>

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

**Sorting results**
You sort the results in tables by clicking a column heading. An arrow at the top of the column indicates the direction of the sort.

**Procedure**
1. Log in to QRadar.
2. Click the column header once to sort the table in descending order; twice to sort the table in ascending order.

**Refreshing and pausing the user interface**
You can manually refresh, pause, and play the data that is displayed on tabs.

**About this task**
The Log Activity tab automatically refreshes every 60 seconds if you are viewing the tab in Last Interval (auto refresh) mode.

The timer, which is on the upper 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 that the current display is paused.

**Procedure**
1. Log in to QRadar.
2. Click the tab that you want to view.
3. Choose one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Click Refresh, on the right corner of the tab, to refresh the tab.</td>
</tr>
</tbody>
</table>
Investigating IP addresses

You can use several methods to investigate information about IP addresses on the Dashboard, Log Activity, and Network Activity tabs.

About this task

You can find more information about an IP address by any of the methods that are listed in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information &gt; DNS Lookup</td>
<td>Searches for DNS entries that are based on the IP address.</td>
</tr>
<tr>
<td>Information &gt; WHOIS Lookup</td>
<td>Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net.</td>
</tr>
<tr>
<td>Information &gt; Port Scan</td>
<td>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.</td>
</tr>
<tr>
<td>Information &gt; Asset Profile</td>
<td>Displays asset profile information. This option is displayed if IBM Security QRadar Vulnerability Manager is purchased and licensed. For more information, see the IBM Security QRadar Vulnerability Manager User Guide. This menu option is available if QRadar acquired profile data actively through a scan.</td>
</tr>
<tr>
<td>Information &gt; Search Events</td>
<td>Searches for events that are associated with this IP address.</td>
</tr>
<tr>
<td>Information &gt; Search Connections</td>
<td>Searches for connections that are associated with this IP address. This option is only displayed if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance. For more information, see the IBM Security QRadar Risk Manager User Guide.</td>
</tr>
</tbody>
</table>

Chapter 2. About QRadar Log Manager 9
Table 5. IP addresses information (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information &gt; View Topology</td>
<td>Displays the tab, which depicts the layer 3 topology of your network. This option is available if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance.</td>
</tr>
<tr>
<td>Information Run &gt; QVM Scan</td>
<td>Select the Run QVM Scan option to scan an IBM Security QRadar Vulnerability Manager scan on this IP address. This option is only displayed when IBM Security QRadar Vulnerability Manager has been purchased and licensed. For more information, see the IBM Security QRadar Vulnerability Manager User Guide.</td>
</tr>
</tbody>
</table>

For information about the Risks tab or IBM Security QRadar Risk Manager, see the IBM Security QRadar Risk Manager User Guide.

**Procedure**
1. Log in to QRadar.
2. Click the tab that you want to view.
3. Move your mouse pointer over an IP address to view the location of the IP address.
4. Right-click the IP address or asset name and select one of the following options:

**Investigate user names**

You can right-click a user name to access more menu options. Use these options to view more information about the user name or IP address.

You can investigate user names when IBM Security QRadar Vulnerability Manager is purchased and licensed. For more information, see the IBM Security QRadar Vulnerability Manager User Guide.

When you right-click a user name, you can choose the following menu options.

Table 6. Menu options for user name investigation

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Assets</td>
<td>Displays current assets that are associated to the selected user name. For more information about viewing assets, see Asset management.</td>
</tr>
<tr>
<td>View User History</td>
<td>Displays all assets that are associated to the selected user name over the previous 24 hours.</td>
</tr>
<tr>
<td>View Events</td>
<td>Displays the events that are associated to the selected user name. For more information about the List of Events window, see Log activity monitoring.</td>
</tr>
</tbody>
</table>
For more information about customizing the right-click menu, see the Administration Guide for your product.

System time

The right corner of the QRadar user interface displays system time, which is the time on the console.

The console time synchronizes QRadar systems within the QRadar deployment. The console time is used to determine what time events were received from other devices for correct time synchronization correlation.

In a distributed deployment, the console might be 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 to specify a time range.

Updating user preferences

You can set your user preference, such as locale, in the main QRadar user interface.

Procedure

1. To access your user information, click Preferences.
2. Update your preferences.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Displays your user name. You cannot edit this field.</td>
</tr>
<tr>
<td>Password</td>
<td>The password must meet the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• Minimum of 6 characters</td>
</tr>
<tr>
<td></td>
<td>• Maximum of 255 characters</td>
</tr>
<tr>
<td></td>
<td>• Contain at least one special character</td>
</tr>
<tr>
<td></td>
<td>• Contain one uppercase character</td>
</tr>
<tr>
<td>Password (Confirm)</td>
<td>Password confirmation,</td>
</tr>
<tr>
<td>Email Address</td>
<td>The email address must meet the following requirements:</td>
</tr>
<tr>
<td></td>
<td>• Minimum of 10 characters</td>
</tr>
<tr>
<td></td>
<td>• Maximum of 255 characters</td>
</tr>
<tr>
<td>Locale</td>
<td>QRadar is available in the following languages: English, Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, Italian, Spanish, Russian and Portuguese (Brazil).</td>
</tr>
<tr>
<td></td>
<td>If a locale is not listed, the user interface is not translated into the associated language. However, other associated cultural conventions, such as, character type, collation, format of date and time, currency unit are supported.</td>
</tr>
<tr>
<td>Enable Popup Notifications</td>
<td>Select this check box if you want to enable pop-up system notifications to be displayed on your user interface.</td>
</tr>
</tbody>
</table>

Chapter 2. About QRadar Log Manager 11
Access online help
You can access the QRadar Online Help through the main QRadar user interface.

To access the Online Help, click **Help > Help Contents**.

Resize columns
You can resize the columns on several tabs in QRadar.

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 work in Microsoft Internet Explorer, Version 7.0 web browsers when tabs are displaying records in streaming mode.

Configure page size
Users with administrative privileges can configure the maximum number of results that display in the tables on various tabs in QRadar.
Chapter 3. Dashboard management

The Dashboard tab is the default view when you log in.

It provides a workspace environment on which you can display your views of the data that is collected.

Dashboards allows you to organize your dashboard items into functional views, which enable you to focus on specific areas of your network.

Use the Dashboard tab to monitor your security event behavior.

You can customize your dashboard. The content that is displayed on the Dashboard tab is user-specific. Changes that are made within a 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 is automatically resized in proportion to the dashboard.
- Add custom dashboard items that are 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 that are 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.

Log activity

The Log Activity dashboard items will 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.
**Table 7. Log activity items**

<table>
<thead>
<tr>
<th>Dashboard item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Searches</td>
<td>You can display a custom dashboard item that is based on saved search criteria from the Log Activity tab. Event search items are listed in the Add Item &gt; Log Activity &gt; Event Searches menu. The name of the event search item matches the name of the saved search criteria the item is based on. QRadar 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. Time series charts are interactive. You can magnify and scan through a timeline to investigate log activity.</td>
</tr>
<tr>
<td>Events By Severity</td>
<td>The Events By Severity dashboard item displays the number of active events that are grouped by severity. This item will allow you to see the number of events that are received by the level of severity assigned. Severity indicates the amount of threat an offense 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.</td>
</tr>
<tr>
<td>Top Log Sources</td>
<td>The Top Log Sources dashboard item displays the top 5 log sources that sent events to QRadar Log Manager within the last 5 minutes. The number of events that are sent from the specified log source is indicated in the pie chart. This item will allow 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.</td>
</tr>
</tbody>
</table>
Most recent reports

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

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 that are received within the last 24 hours.

Vulnerability Management items

Vulnerability Management dashboard items are only displayed when IBM Security QRadar Vulnerability Manager is purchased and licensed.

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

You can display a custom dashboard item that is 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 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.

System notification

The Systems Notification dashboard item displays event notifications that are received by your system.

For notifications to show in the System Notification dashboard item, the Administrator must create a rule that is 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 Guide.

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

- Flag - Displays a symbol to indicate severity level of the notification. Point to 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 elapsed since the notification was created.
- **Description** - Displays information about the notification.
- **Dismiss icon (x)** - Will allow you to close 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 that is associated with the incident that generated this notification. For example: Service Disruption.
- **Payload** - Displays the payload content that is associated with the incident that generated this notification.
- **Created** - Displays the amount of time 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 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.

In the System Notifications pop-up window, the number of notifications in the queue is highlighted. For example, if (1 - 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 more information about this system notification.

---

**Adding dashboard items**

You can add multiple dashboard items to your Dashboard tab.

**Procedure**

1. Click the **Dashboard** tab.
2. From the toolbar, click **Add Item**.
3. Select the item you want to add. See Available dashboard items.

---

**Using the dashboard to investigate log activity**

Search-based dashboard items provide a link to the **Log Activity** tab, allowing you to further investigate log activity.
About this task

To investigate flows from a Log Activity dashboard item:

1. Click the View in Log Activity link. The Log Activity tab is displayed, displaying results and two charts that match the parameters of your dashboard item.

The chart types that are displayed on the Log activity tab depend on which chart is configured in the dashboard item:

<table>
<thead>
<tr>
<th>Chart type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar, Pie, and Table</td>
<td>The Log Activity tab displays a bar chart, pie chart, and table of details.</td>
</tr>
<tr>
<td>Time Series</td>
<td>The Log Activity tab displays charts according to the following criteria: 1. 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. 2. 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.</td>
</tr>
</tbody>
</table>

Configuring charts

You can configure Log Activity, Network Activity, and Connections (if applicable) dashboard items to specify the chart type and how many data objects you want to view.

About this task

Table 8. Configuring Charts. Parameter options.

<table>
<thead>
<tr>
<th>option</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value to Graph</td>
<td>From the list box, select the object type that you want to graph on the chart. Options include all normalized and custom event or flow parameters included in your search parameters.</td>
</tr>
</tbody>
</table>
Table 8. Configuring Charts (continued). Parameter options.

<table>
<thead>
<tr>
<th>option</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chart Type</td>
<td>From the list box, select the chart type that you want to view. Options include:</td>
</tr>
<tr>
<td></td>
<td>1. <strong>Bar Chart</strong> - Displays data in a bar chart. This option is only available for grouped events.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Pie Chart</strong> - Displays data in a pie chart. This option is only available for grouped events.</td>
</tr>
<tr>
<td></td>
<td>3. <strong>Table</strong> - Displays data in a table. This option is only available for grouped events.</td>
</tr>
<tr>
<td></td>
<td>4. <strong>Time Series</strong> - Displays an interactive line chart that represents the records that are matched by a specified time interval.</td>
</tr>
<tr>
<td>Display Top</td>
<td>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.</td>
</tr>
<tr>
<td>Capture Time Series Data</td>
<td>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.</td>
</tr>
<tr>
<td>Time Range</td>
<td>From the list box, select the time range that you want to view.</td>
</tr>
</tbody>
</table>

Your custom chart configurations are retained, so that they are displayed as configured each time that you access the **Dashboard** tab.

QRadar Log Manager collects data so that when you perform a time series saved search, there is a cache of event or flow 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.

**Procedure**

1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard that contains the item you want to customize.
3. On the header of the dashboard item you want to configure, click the **Settings** icon.
4. Configure the chart parameters that are described in Table 1.

**Removing dashboard items**

You can remove items from a dashboard and add the item again at any time.

**About this task**

When you remove an item from the dashboard, the item is not removed completely.
Procedure
1. Click the Dashboard tab.
2. From the Show Dashboard list box, select the dashboard from which you want to remove an item.
3. On the dashboard item header, click the red [x] icon to remove the item from the dashboard.

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

About this task
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 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
1. Click the Dashboard tab.
2. From the Show Dashboard list box, select the dashboard from which you want to detach an item.
3. On the dashboard item header, click the green icon to detach the dashboard item and open it in separate window.

Renaming a dashboard
You can rename a dashboard and update the description.

Procedure
1. Click the Dashboard tab.
2. From the Show Dashboard list box, select the dashboard that you want to edit.
3. On the toolbar, click the Rename Dashboard icon.
4. In the Name field, type a new name for the dashboard. The maximum length is 65 characters.
5. In the Description field, type a new description of the dashboard. The maximum length is 255 characters.
6. Click OK.

Deleting a dashboard
You can delete a dashboard.

About this task
After you delete a dashboard, the Dashboard tab refreshes and the first dashboard that is listed in the Show Dashboard list box is displayed. The dashboard that you deleted is no longer displayed in the Show Dashboard list box.
**Procedure**
1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard that you want to delete.
3. On the toolbar, click **Delete Dashboard**.
4. Click **Yes**.

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

**Before you begin**
Ensure the **System Notification** dashboard item is added to your dashboard.

**Procedure**
1. On the System Notification dashboard item header, click the **Settings** icon.
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 that are logged in the past 24 hours, click **All**.
3. To close a system notification, click the **Delete** icon.

**Adding search-based dashboard items to the Add Items list**
You can add search-based dashboard items to your **Add Items** menu.

**Before you begin**
To add an event dashboard item to the **Add Item** menu on the **Dashboard** tab, you must access the **Log 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.

**About this task**
This procedure applies to all search-based dashboard items, including IBM Security QRadar Risk Manager dashboard items. QRadar Risk Manager dashboard items are only displayed when QRadar Risk Manager was purchased and licensed, and you established the connection between the Console and the QRadar Risk Manager appliance. For more information, see the *IBM Security QRadar Risk Manager User Guide*.

**Procedure**
1. Choose:
   - To add an event search dashboard item, click the **Log Activity** tab.
2. From the **Search** list box, choose one of the following options:
   - To create a search, select **New Search**.
   - To edit a saved search, select **Edit Search**.
3. Configure or edit your search parameters, as required.
   - 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.

4. Click Filter. The search results are displayed.
5. Click Save Criteria. See Saving search criteria on the Offense tab
6. Click OK.
7. Verify that your saved search criteria successfully added the event or flow search dashboard item to the Add Items list
8. Click the Dashboard tab.
9. To verify an event search item, select Add Item > Log Activity > Event Searches > Add Item
Chapter 4. Log activity investigation

You can monitor and investigate log activity (events) in real-time or perform advanced searches.

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.

Log activity tab toolbar

You can access several options from the Log Activity toolbar

Using the toolbar, you can access the following options:

<table>
<thead>
<tr>
<th>Table 9. Log Activity toolbar options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>Search</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Quick Searches</td>
</tr>
<tr>
<td>Add Filter</td>
</tr>
<tr>
<td>Save Criteria</td>
</tr>
<tr>
<td>Save Results</td>
</tr>
<tr>
<td>Cancel</td>
</tr>
</tbody>
</table>
Table 9. Log Activity toolbar options  (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Rules  | The Rules option is only visible if you have permission to view rules. Click Rules to configure custom event rules. Options include:  
- **Rules** - Select this option to view or create a rule. If you only have the permission to view rules, the summary page of the Rules wizard is displayed. If you have the permission to maintain custom rules, the Rules wizard is displayed and you can edit the rule. To enable the anomaly detection rule options (Add Threshold Rule, Add Behavioral Rule, and Add Anomaly Rule), you must save aggregated search criteria because the saved search criteria specifies the required parameters.  
**Note:** The anomaly detection rule options are only visible if you have the Log Activity > Maintain Custom Rules permission.  
- **Add Threshold Rule** - Select this option to create a threshold rule. A threshold rule tests event traffic for activity that exceeds a configured threshold. Thresholds can be based on any data that is collected QRadar. For example, if you create a threshold rule indicating that no more than 220 clients can log in to the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to log in.  
When you select the Add Threshold Rule option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a threshold rule. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules (continued)</td>
<td>• <strong>Add Behavioral Rule</strong> - Select this option to create a behavioral rule. A behavioral rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, you can create a behavioral rule to compare the average volume of traffic for the last 5 minutes with the average volume of traffic over the last hour. If there is more than a 40% change, the rule generates a response.</td>
</tr>
<tr>
<td></td>
<td>When you select the <strong>Add Behavioral Rule</strong> option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a behavioral rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add Anomaly Rule</strong> - Select this option to create an anomaly rule. An anomaly rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, if an area of your network that never communicates with Asia starts communicating with hosts in that country, an anomaly rule generates an alert.</td>
</tr>
<tr>
<td></td>
<td>When you select the <strong>Add Anomaly Rule</strong> option, the Rules wizard is displayed, prepopulated with the appropriate options for creating an anomaly rule.</td>
</tr>
</tbody>
</table>
### Table 9. Log Activity toolbar options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td><strong>Actions</strong> to perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Show All</strong> - Select this option to remove all filters on search criteria and display all unfiltered events.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Print</strong> - Select this option to print the events that are displayed on the page.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Export to XML &gt; Visible Columns</strong> - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Export to XML &gt; Full Export (All Columns)</strong> - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Export to CSV &gt; Visible Columns</strong> - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Export to CSV &gt; Full Export (All Columns)</strong> - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Delete</strong> - Select this option to delete a search result. See Managing event and flow search results.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Notify</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <strong>Print</strong>, <strong>Export to XML</strong>, and <strong>Export to CSV</strong> options are disabled in streaming mode and when viewing partial search results.</td>
</tr>
<tr>
<td>Quick Filter</td>
<td>Type your search criteria in the <strong>Quick Filter</strong> field and click the <strong>Quick Filter</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you click the <strong>Quick Filter</strong> field, a tooltip is displayed, providing information about the appropriate syntax to use for search criteria. For more syntax information, see <strong>Quick Filter syntax</strong>.</td>
</tr>
</tbody>
</table>
Quick filter syntax

The Quick Filter feature will enable you to search event payloads by 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 will enable 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, which is 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 will enable 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 page - From the event search page, 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 or flows](#).

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 by 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 quotation marks to indicate that you want to search for the exact phrase. For example, "Firewall deny"

- Search terms can include single and multiple character wildcards. The search term cannot start with a wildcard. 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" does not match the following phrases: "ruser", "myuser", or "anyuser". The search term "user*" does match any word that begins with "user", for example, "user_1", "user_2".

- Group terms by using logical expressions, such as AND, OR, and NOT. The syntax is case-sensitive and the operators must be uppercase 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 you create 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 more event filter information.

The right-click menu options are:
### Table 10. Right-click menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter on</td>
<td>Select this option to filter on the selected event, depending on the selected parameter in the event.</td>
</tr>
<tr>
<td>More options:</td>
<td>Select this option to investigate an IP address or a user name. For more information about investigating an IP address, see Investigating IP addresses. For more information about investigating a user name, see Investigating user names. <strong>Note:</strong> This option is not displayed in streaming mode.</td>
</tr>
</tbody>
</table>

### Status bar

When streaming events, the status bar displays the average number of results that are 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 more status information, move your mouse pointer over the status bar.

When events are not being streamed, the status bar displays the number of search results that are currently displayed on the tab and the amount of time that is required to process the search results.

### Log activity monitoring

By default, the **Log Activity** tab displays events in streaming mode, which allow 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 by 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 and flow search criteria.

### Viewing streaming events

Streaming mode will enable you to view event data that enters 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 the streaming is paused, the last 1,000 events are displayed.

**Procedure**
1. Click the Log Activity tab.
2. From the View list box, select Real Time (streaming). For information about the toolbar options, see Table 4-1. For more information about the parameters that are displayed in streaming mode, see Table 4-7.
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**
Events are collected in raw format, and then normalized for display on the Log Activity tab.

**About this task**
Normalization involves parsing raw event data and preparing the data to display readable information about the tab. When events are normalized, the system normalizes the 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 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 11. Log Activity tab - Default (Normalized) parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current® Filters</td>
<td>The top of the table displays the details of the filters that are applied to the search results. To clear these filter values, click Clear Filter. Note: This parameter is only displayed after you apply a filter.</td>
</tr>
<tr>
<td>View</td>
<td>From this list box, you can select the time range that you want to filter for.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Current Statistics</strong></td>
<td>When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including:</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Click the arrow next to <strong>Current Statistics</strong> to display or hide the statistics</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total Results</strong> - Specifies the total number of results that matched your search criteria.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Data Files Searched</strong> - Specifies the total number of data files searched during the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Compressed Data Files Searched</strong> - Specifies the total number of compressed data files searched within the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Index File Count</strong> - Specifies the total number of index files searched during the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Duration</strong> - Specifies the duration of the search.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.</td>
</tr>
<tr>
<td><strong>Charts</strong></td>
<td>Displays configurable charts that represent the records that are matched by the time interval and grouping option. Click <strong>Hide Charts</strong> 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 <strong>Chart management</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td><strong>Offenses icon</strong></td>
<td>Click this icon to view details of the offense that is associated with this event. For more information, see <strong>Chart management</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Depending on your product, this icon is might not be available. You must have IBM Security QRadar SIEM.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Specifies the time of the first event, as reported to QRadar by the log source.</td>
</tr>
<tr>
<td><strong>Event Name</strong></td>
<td>Specifies the normalized name of the event.</td>
</tr>
</tbody>
</table>
### Table 11. Log Activity tab - Default (Normalized) parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source</td>
<td>Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.</td>
</tr>
<tr>
<td>Event Count</td>
<td>Specifies the total number of events that are 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 time.</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies the date and time when QRadar received the event.</td>
</tr>
<tr>
<td>Low Level Category</td>
<td>Specifies the low-level category that is associated with this event. For more information about event categories, see the IBM Security QRadar Log Manager Administration Guide.</td>
</tr>
<tr>
<td>Source IP</td>
<td>Specifies the source IP address of the event.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specifies the source port of the event.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Specifies the destination IP address of the event.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies the destination port of the event.</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the user name that is 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.</td>
</tr>
<tr>
<td>Magnitude</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Procedure

1. Click the Log Activity tab.
2. From the Display list box, select Default (Normalized).
3. From the View list box, select the time frame that you want to display.
4. Click the Pause icon to pause streaming.
5. Double-click the event that you want to view in greater detail. For more information, 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 12. Raw Event parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Filters</td>
<td>The top of the table displays the details of the filters that are applied to the search results. To clear these filter values, click Clear Filter. Note: This parameter is only displayed after you apply a filter.</td>
</tr>
<tr>
<td>View</td>
<td>From this list box, you can select the time range that you want to filter for.</td>
</tr>
<tr>
<td>Current Statistics</td>
<td>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.</td>
</tr>
<tr>
<td>Charts</td>
<td>Displays configurable charts that represent the records that are 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. 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.</td>
</tr>
</tbody>
</table>
Table 12. Raw Event parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Specifies the time of the first event, as reported to QRadar by the log source.</td>
</tr>
<tr>
<td>Log Source</td>
<td>Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.</td>
</tr>
<tr>
<td>Payload</td>
<td>Specifies the original event payload information in UTF-8 format.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Click the **Log Activity** tab.
2. From the **Display** list box, select **Raw Events**.
3. From the **View** list box, select the time frame that you want to display.
4. Double-click the event that you want to view in greater detail. See **Event details**.

**Viewing grouped events**

Using the **Log Activity** tab, you can view events that are 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 by using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

**Table 13. Grouped events options**

<table>
<thead>
<tr>
<th>Group option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Level Category</td>
<td>Displays a summarized list of events that are grouped by the low-level category of the event.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Displays a summarized list of events that are grouped by the normalized name of the event.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Displays a summarized list of events that are grouped by the destination IP address of the event.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Displays a summarized list of events that are grouped by the destination port address of the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>Displays a summarized list of events that are grouped by the source IP address of the event.</td>
</tr>
<tr>
<td>Custom Rule</td>
<td>Displays a summarized list of events that are grouped by the associated custom rule.</td>
</tr>
</tbody>
</table>
Table 13. Grouped events options (continued)

<table>
<thead>
<tr>
<th>Group option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Displays a summarized list of events that are grouped by the user name that is associated with the events.</td>
</tr>
<tr>
<td>Log Source</td>
<td>Displays a summarized list of events that are grouped by the log sources that sent the event to QRadar.</td>
</tr>
<tr>
<td>High Level Category</td>
<td>Displays a summarized list of events that are grouped by the high-level category of the event.</td>
</tr>
<tr>
<td>Network</td>
<td>Displays a summarized list of events that are grouped by the network that is associated with the event.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Displays a summarized list of events that are grouped by the source port address of the event.</td>
</tr>
</tbody>
</table>

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 14. Grouped event parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping By</td>
<td>Specifies the parameter that the search is grouped on.</td>
</tr>
<tr>
<td>Current Filters</td>
<td>The top of the table displays the details of the filter that is applied to the search results. To clear these filter values, click <strong>Clear Filter</strong>.</td>
</tr>
<tr>
<td>View</td>
<td>From the list box, select the time range that you want to filter for.</td>
</tr>
</tbody>
</table>
Table 14. Grouped event parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Statistics</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total Results</strong> - Specifies the total number of results that matched your search criteria.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Data Files Searched</strong> - Specifies the total number of data files searched during the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Compressed Data Files Searched</strong> - Specifies the total number of compressed data files searched within the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Index File Count</strong> - Specifies the total number of index files searched during the specified time span.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Duration</strong> - 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.</td>
</tr>
</tbody>
</table>
### Table 14. Grouped event parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Charts                     | Displays configurable charts that represent the records that are 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.  
  - 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.  
  *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 that is associated with this event. If there are multiple IP addresses that are 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 that is associated with this event. If there are multiple IP addresses that are associated with this event, this field specifies the term *Multiple* and the number of IP addresses. |
| Destination Port (Unique Count) | Specifies the destination ports that are associated with this event. If there are multiple ports that are associated with this event, this field specifies the term *Multiple* and the number of ports. |
| Event Name                 | Specifies the normalized name of the event.                                                                                                                                                    |
### Table 14. Grouped event parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source (Unique Count)</td>
<td>Specifies the log sources that sent the event to QRadar. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.</td>
</tr>
<tr>
<td>High Level Category (Unique Count)</td>
<td>Specifies the high-level category of this event. If there are multiple categories that are 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.</td>
</tr>
<tr>
<td>Low Level Category (Unique Count)</td>
<td>Specifies the low-level category of this event. If there are multiple categories that are associated with this event, this field specifies the term Multiple and the number of categories.</td>
</tr>
<tr>
<td>Protocol (Unique Count)</td>
<td>Specifies the protocol ID associated with this event. If there are multiple protocols that are associated with this event, this field specifies the term Multiple and the number of protocol IDs.</td>
</tr>
<tr>
<td>Username (Unique Count)</td>
<td>Specifies the user name that is associated with this event, if available. If there are multiple user names that are associated with this event, this field specifies the term Multiple and the number of user names.</td>
</tr>
<tr>
<td>Magnitude (Maximum)</td>
<td>Specifies the maximum calculated magnitude for grouped events. Variables that are used to calculate magnitude include credibility, relevance, and severity. For more information about credibility, relevance, and severity, see the <a href="#">Glossary</a>.</td>
</tr>
<tr>
<td>Event Count (Sum)</td>
<td>Specifies the total number of events that are 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 time.</td>
</tr>
<tr>
<td>Count</td>
<td>Specifies the total number of normalized events in this event group.</td>
</tr>
</tbody>
</table>

### Procedure

1. Click the **Log Activity** tab.
2. From the **View** list box, select the time frame that you want to display.
3. From the **Display** list box, choose which parameter you want to group events on. See Table 2. The events groups are listed. For more information about the event group details, see Table 1.
4. To view the List of Events page for a group, double-click the event group that you want to investigate. The List of Events page does not retain chart configurations that you might have defined on the **Log Activity** tab. For more information about the List of Events page parameters, see Table 1.
5. To view the details of an event, double-click the event that you want to investigate. For more information about event details, see Table 2.

**Event details**

You can view a list of events 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 15. Event details*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Specifies the normalized name of the event.</td>
</tr>
<tr>
<td>Low Level Category</td>
<td>Specifies the low-level category of this event.</td>
</tr>
<tr>
<td>Event Description</td>
<td>Specifies a description of the event, if available.</td>
</tr>
<tr>
<td>Magnitude</td>
<td>Specifies the magnitude of this event. For more information about magnitude, see the Glossary</td>
</tr>
<tr>
<td>Relevance</td>
<td>Specifies the relevance of this event. For more information about relevance, see the Glossary</td>
</tr>
<tr>
<td>Severity</td>
<td>Specifies the severity of this event. For more information about severity, see the Glossary</td>
</tr>
<tr>
<td>Credibility</td>
<td>Specifies the credibility of this event. For more information about credibility, see the Glossary</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the user name that is associated with this event, if available.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Specifies the time of the event was received from the log source.</td>
</tr>
<tr>
<td>Storage Time</td>
<td>Specifies the time that the event was stored in the QRadar database.</td>
</tr>
<tr>
<td>Log Source Time</td>
<td>Specifies the system time as reported by the log source in the event payload.</td>
</tr>
</tbody>
</table>

**Source and Destination information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Specifies the source IP address of the event.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Specifies the destination IP address of the event.</td>
</tr>
<tr>
<td>Source Asset Name</td>
<td>Specifies the user-defined asset name of the event source. For more information about assets, see Asset management.</td>
</tr>
<tr>
<td>Destination Asset Name</td>
<td>Specifies the user-defined asset name of the event destination. For more information about assets, see Asset management</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specifies the source port of this event.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies the destination port of this event.</td>
</tr>
<tr>
<td>Pre NAT Source IP</td>
<td>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.</td>
</tr>
<tr>
<td>Pre NAT Destination IP</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the destination IP address before the NAT values were applied.</td>
</tr>
<tr>
<td>Pre NAT Source Port</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the source port before the NAT values were applied.</td>
</tr>
<tr>
<td>Pre NAT Destination Port</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the destination port before the NAT values were applied.</td>
</tr>
<tr>
<td>Post NAT Source IP</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the source IP address after the NAT values were applied.</td>
</tr>
<tr>
<td>Post NAT Destination IP</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the destination IP address after the NAT values were applied.</td>
</tr>
<tr>
<td>Post NAT Source Port</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.</td>
</tr>
<tr>
<td>Post NAT Destination Port</td>
<td>For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.</td>
</tr>
<tr>
<td>IPv6 Source</td>
<td>Specifies the source IPv6 address of the event.</td>
</tr>
<tr>
<td>IPv6 Destination</td>
<td>Specifies the destination IPv6 address of the event.</td>
</tr>
<tr>
<td>Source MAC</td>
<td>Specifies the source MAC address of the event.</td>
</tr>
<tr>
<td>Destination MAC</td>
<td>Specifies the destination MAC address of the event.</td>
</tr>
</tbody>
</table>

Payload information
### Table 15. Event details (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Payload**             | Specifies the payload content from the event. This field offers 3 tabs to view the payload:  
|                         | • Universal Transformation Format (UTF) - Click UTF.                        |
|                         | • Hexadecimal - Click HEX.                                                  |
|                         | • Base64 - Click Base64.                                                    |
| **Additional information** |                                                                               |
| **Protocol**            | Specifies the protocol that is 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. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources. |
| **Event Count**         | Specifies the total number of events that are 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 time. |
| **Custom Rules**        | Specifies custom rules that match this event.                              |
| **Custom Rules Partially Matched** | Specifies custom rules that partially match this event.                     |
| **Annotations**         | Specifies the annotation for this event. Annotations are text descriptions that rules can automatically add to events as part of the rule response. |

**Identity information** - QRadar collects identity information, if available, from log source messages. Identity information provides extra details about assets on your network. Log sources only generate identity information if the log message sent to QRadar contains an IP address and at least one of the following items: User name or MAC address. Not all log sources generate identity information. For more information about identity and assets, see Asset management.

| Identity Username       | Specifies the user name of the asset that is associated with this event.    |
| Identity IP             | Specifies the IP address of the asset that is associated with this event.   |
| Identity Net Bios Name  | Specifies the Network Base Input/Output System (Net Bios) name of the asset that is associated with this event. |
### Table 15. Event details (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Extended field</strong></td>
<td>Specifies more information about the asset that is 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.</td>
</tr>
<tr>
<td>Has Identity (Flag)</td>
<td>Specifies True if QRadar has collected identify information for the asset that is associated with this event. For more information about which devices send identity information, see the IBM Security QRadar DSM Configuration Guide.</td>
</tr>
<tr>
<td>Identity Host Name</td>
<td>Specifies the host name of the asset that is associated with this event.</td>
</tr>
<tr>
<td>Identity MAC</td>
<td>Specifies the MAC address of the asset that is associated with this event.</td>
</tr>
<tr>
<td>Identity Group Name</td>
<td>Specifies the group name of the asset that is associated with this event.</td>
</tr>
</tbody>
</table>

### Event details toolbar

The events details toolbar provides several functions for viewing events detail.

The **event details** toolbar provides the following functions:

**Table 16. Event details toolbar**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to Events List</td>
<td>Click <strong>Return to Events List</strong> to return to the list of events.</td>
</tr>
<tr>
<td>Map Event</td>
<td>Click <strong>Map Event</strong> to edit the event mapping. For more information, see <a href="https://www.ibm.com/support/knowledgecenter/SSSUGY_3.2.0/com.ibm.qradar.doc/">Modifying event mapping</a>.</td>
</tr>
<tr>
<td>False Positive</td>
<td>Click <strong>False Positive</strong> to tune QRadar to prevent false positive events from generating into offenses.</td>
</tr>
<tr>
<td>Extract Property</td>
<td>Click <strong>Extract Property</strong> to create a custom event property from the selected event.</td>
</tr>
<tr>
<td>Previous</td>
<td>Click <strong>Previous</strong> to view the previous event in the event list.</td>
</tr>
<tr>
<td>Next</td>
<td>Click <strong>Next</strong> to view the next event in the event list.</td>
</tr>
</tbody>
</table>
Table 16. Event details toolbar (continued)

<table>
<thead>
<tr>
<th>PCAP Data</th>
<th>Note: This option is only displayed if your QRadar Console is configured to integrate with the Juniper JunOS Platform DSM. For more information about managing PCAP data, see Managing PCAP data.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>View PCAP Information</strong> - Select this option to view the PCAP information. For more information, see Viewing PCAP information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Download PCAP File</strong> - Select this option to download the PCAP file to your desktop system. For more information, see Downloading the PCAP file to your desktop system.</td>
</tr>
<tr>
<td>Print</td>
<td>Click <strong>Print</strong> to print the event details.</td>
</tr>
</tbody>
</table>

### Modifying event mapping

You can manually map a normalized or raw event to a high-level and low-level category (or QID).

#### Before you begin

This manual action is used to map unknown log source events to known QRadar events so that they can be categorized and processed appropriately.

#### About this task

For normalization purposes, QRadar 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*.

If events are received from log sources that the system is unable to categorize, then the events are categorized as unknown. These events occur for several reasons, including:

- **User-defined Events** - Some log sources, such as Snort, allows 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 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

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event that you want to map.
4. Click **Map Event**.
5. If you know the QID that you want to map to this event, type the QID in the **Enter QID** field.

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

7. Click **OK**.

---

### Managing PCAP data

If your QRadar Console is configured to integrate with the Juniper JunOS Platform DSM, then Packet Capture (PCAP) can be received, processed, and data can be stored 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 *Managing Log Sources 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**

1. Click the **Log Activity** tab.
2. From the **Search** list box, select **New Search**.
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**.
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.

5. Click Filter.

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

7. Double-click the event that 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 a readable version of the data in the PCAP file or download the PCAP file to your desktop system.

Before you begin

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

About this task

Before PCAP data can be displayed, the PCAP file must be retrieved for display on the user interface. If the download process takes an extended period, 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 that is displayed on the window, or download the information to your desktop system.

Procedure

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 that you want to investigate, and then select PCAP Data > View PCAP Information from the event details toolbar.

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.

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.

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**

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.

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.

3. Click **OK**.

**Exporting events**

You can export events in Extensible Markup Language (XML) or Comma-Separated Values (CSV) format.

**Before you begin**

The length of time that is required to export your data depends on the number of parameters specified.

**Procedure**

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
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.

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

Results

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.
Chapter 5. Chart management

You can use various chart configuration options to view your data.

If you select a time frame or a grouping option to view your data, then the 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 that represents the records that are matched by a specified time interval. For information about 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 by 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 activity over time.

Peaks and valleys that are 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 or network activity from various views and perspectives.
Note: You must have the appropriate role permissions to manage and view time series charts.

To display time series charts, you must create and save a search that includes time series and grouping options. You can save up to 100 time series searches.

Default time series saved searches are accessible 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 timeline on a time series chart to investigate activity. The following table provides functions that you can use to view time series charts.

Table 17. Time series charts functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View data in greater detail</td>
<td>Using the zoom feature, you can investigate smaller time segments of event traffic.</td>
</tr>
<tr>
<td></td>
<td>Move your mouse pointer over the chart, and then use your mouse wheel to magnify the chart (roll the mouse wheel up).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When you magnify a time series chart, the chart refreshes to display a smaller time segment.</td>
</tr>
<tr>
<td>View a larger time span of data</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>Click Zoom Reset at the upper left corner of the chart.</td>
</tr>
<tr>
<td></td>
<td>Move your mouse pointer over the chart, and then use your mouse wheel to expand the view (roll the mouse wheel down).</td>
</tr>
<tr>
<td>Scan the chart</td>
<td>When you have magnified a time series chart, you can click and drag the chart to the left or right to scan the timeline.</td>
</tr>
</tbody>
</table>
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.
- 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 that are represented on the chart. For time series charts, you can also select a time range and enable time series data capture.

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 and flow search criteria.
- On the toolbar, select a saved search from the Quick Search list.
- Perform a grouped search, and then click Save Criteria on the toolbar.

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

About this task

Data can be accumulated 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.

Procedure

1. Click the Log Activity tab.
2. In the Charts pane, click the Configure icon.
3. Configure values the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value to Graph</td>
<td>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.</td>
</tr>
<tr>
<td>Display Top</td>
<td>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.</td>
</tr>
<tr>
<td>Chart Type</td>
<td>From the list box, select the chart type that you want to view.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Capture Time Series Data</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This option is only available on Time Series charts.</td>
</tr>
<tr>
<td>Time Range</td>
<td>From the list box, select the time range that you want to view.</td>
</tr>
<tr>
<td></td>
<td>This option is only available on Time Series charts.</td>
</tr>
</tbody>
</table>

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

5. To view the list of events if your time range is greater than 1 hour, click **Update Details**.
Chapter 6. Data searches

On the Log Activity tab, you can search events by using specific criteria.

You can create a 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.

After you perform a search, you can save the search criteria and the search results.

Searching for items that match your criteria

You can search for data that matches your search criteria.

About this task

Since the entire database is searched, searches might take an extended time, depending on the size of your database.

You can use the Quick Filter search parameter to search for items that match your text string in the event payload.

For more information about how to use the Quick Filter parameter, see Quick Filter syntax (events).

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

Table 18. Search options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select an event search group to view in the Available Saved Searches list.</td>
</tr>
<tr>
<td>Type Saved Search or Select from List</td>
<td>Type the name of a saved search or a keyword to filter the Available Saved Searches list.</td>
</tr>
<tr>
<td>Available Saved Searches</td>
<td>This list displays all available searches, unless you use Group or Type Saved Search or Select from List options to apply a filter to the list. You can select a saved search on this list to display or edit.</td>
</tr>
<tr>
<td>Search</td>
<td>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.</td>
</tr>
<tr>
<td>Include in my Quick Searches</td>
<td>Select this check box to include this search in your Quick Search menu.</td>
</tr>
<tr>
<td>Include in my Dashboard</td>
<td>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.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set as Default</td>
<td>Select this check box to set this search as your default search.</td>
</tr>
<tr>
<td>Share with Everyone</td>
<td>Select this check box to share this search with all other users.</td>
</tr>
<tr>
<td>Real Time (streaming)</td>
<td>Displays results in streaming mode. For more information about streaming mode, see Viewing streaming events.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>Last Interval (auto refresh)</td>
<td>Displays the search results in auto-refresh mode.</td>
</tr>
<tr>
<td></td>
<td>In auto-refresh mode, the Log Activity tab refresh at one-minute interval to display the most recent information.</td>
</tr>
<tr>
<td>Recent</td>
<td>Select a predefined time range for your search. After you select this option, you must select a time range option from the list box.</td>
</tr>
<tr>
<td>Specific Interval</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 18. Search options (continued)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Accumulation</td>
<td>This pane is only displayed when you load a saved search.</td>
</tr>
<tr>
<td></td>
<td>Enabling unique counts on accumulated data that is shared with many other saved searches and reports might decrease system performance.</td>
</tr>
<tr>
<td></td>
<td>When you load a saved search, this pane displays the following options:</td>
</tr>
<tr>
<td></td>
<td>• If no data is accumulating for this saved search, the following information message is displayed: Data is not being accumulated for this search.</td>
</tr>
<tr>
<td></td>
<td>• If data is accumulating for this saved search, the following options are displayed:</td>
</tr>
<tr>
<td></td>
<td>  columns - When you click or hover your mouse over this link, a list of the columns that are accumulating data opens.</td>
</tr>
<tr>
<td></td>
<td>  Enable Unique Counts/Disable Unique Counts - This link allows you to enable or disable the search results to display unique event counts instead</td>
</tr>
<tr>
<td></td>
<td> 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</td>
</tr>
<tr>
<td></td>
<td> accumulated data.</td>
</tr>
<tr>
<td>Current Filters</td>
<td>This list displays the filters that are applied to this search. The options to add a filter are located above Current Filters list.</td>
</tr>
<tr>
<td>Save results when the search is complete</td>
<td>Select this check box to save and name the search results.</td>
</tr>
<tr>
<td>Display</td>
<td>Select this list to specify a predefined column that is set to display in the search results.</td>
</tr>
<tr>
<td>Type Column or Select from List</td>
<td>You can use field to filter the columns that are listed in the Available Columns list.</td>
</tr>
<tr>
<td></td>
<td>Type the name of the column that you want to locate or type a keyword to display a list of column names. For example, type Device to display a list</td>
</tr>
<tr>
<td></td>
<td> of columns that include Device in the column name.</td>
</tr>
<tr>
<td>Available Columns</td>
<td>This list displays available columns. Columns that are currently in use for this saved search are highlighted and displayed in the Columns list.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add and remove column icons (top set)</td>
<td>Use the top set of icons to customize the Group By list.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Add Column</strong> - Select one or more columns from the Available Columns list and click the <strong>Add Column</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Remove Column</strong> - Select one or more columns from the <strong>Group By</strong> list and click the <strong>Remove Column</strong> icon.</td>
</tr>
<tr>
<td>Add and remove column icons (bottom set)</td>
<td>Use the bottom set of icon to customize the Columns list.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Add Column</strong> - Select one or more columns from the Available Columns list and click the <strong>Add Column</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Remove Column</strong> - Select one or more columns from the Columns list and click the <strong>Remove Column</strong> icon.</td>
</tr>
<tr>
<td>Group By</td>
<td>This list specifies the columns on which the saved search groups the results. Use the following options to customize the Group By list further:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move Up</strong> - Select a column and move it up through the priority list using the <strong>Move Up</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move Down</strong> - Select a column and move it down through the priority list using the <strong>Move Down</strong> icon.</td>
</tr>
<tr>
<td></td>
<td>The priority list specifies in which order the results are grouped. The search results are grouped by the first column in the <strong>Group By</strong> list and then grouped by the next column on the list.</td>
</tr>
<tr>
<td>Columns</td>
<td>Specifies columns that are 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:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move Up</strong> - Moves the selected column up the priority list.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move Down</strong> - Moves the selected own the priority list.</td>
</tr>
<tr>
<td></td>
<td>If the column type is numeric or time-based and there is an entry in the <strong>Group By</strong> list, then the column includes a list box. Use the list box to choose how you want to group the column.</td>
</tr>
<tr>
<td></td>
<td>If the column type is group, the column includes a list box to choose how many levels you want to include for the group.</td>
</tr>
</tbody>
</table>
### Table 18. Search options (continued)

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order By</td>
<td>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 that you want to display for the search results. Options include <em>Descending</em> and <em>Ascending</em>.</td>
</tr>
</tbody>
</table>
| Results Limit | You can specify the number of rows a search returns on the Edit Search window. The **Results Limit** field also appears on the Results window.  
- For a saved search, the limit is stored in the saved search and re-applied when loading the search.  
- When sorting on a column in the search result that has row limit, sorting is done within the limited rows shown in the data grid.  
- For a grouped by search with time series chart turned on, the row limit only applies to the data grid. The **Top N** dropdown in the time series chart still controls how many time series are drawn in the chart. |

### Procedure

1. Click the **Log Activity** tab.
2. From the **Search** list box, select **New Search**.
3. To 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 that you want for this search. See Table 1.
4. To create a search, in the Time Range pane, select the options for the time range you want to capture for this search.
5. 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 about enabling unique counts, see Table 1.
6. In the Search Parameters pane, define your search criteria:
   a. From the first list box, select a parameter that you want to search for. For example, Device, Source Port, or Event Name.
   b. From the second list box, select the modifier that you want to use for the search.
   c. In the entry field, type specific information that is 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.

7. 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.

8. 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 that is 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 1.
   d. Optional. In the Results Limit field, type the number of rows that you want the search to return.

9. Click Filter.

Results

The In Progress (<percent>%Complete) status is displayed in the upper 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 upper right corner.

Saving search criteria

You can save configured search criteria so that you can reuse the criteria and use the saved search criteria in other components, such as reports. Saved search criteria does not expire.

About this task

If you specify a time range for your search, then your search name is appended 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

1. Click the Log Activity tab.
2. Perform a search.
3. Click Save Criteria.
4. Enter values for the parameters:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Description</td>
<td></td>
</tr>
<tr>
<td>Search Name</td>
<td>Type the unique name that you want to assign to this search criteria.</td>
</tr>
<tr>
<td>Assign Search to Group(s)</td>
<td>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 <a href="#">Managing search groups</a>.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>Click <a href="#">Manage Groups</a> to manage search groups. For more information, see <a href="#">Managing search groups</a>.</td>
</tr>
<tr>
<td>Timespan options:</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td>Real Time (streaming)</td>
<td>- Select this option to filter your search results while in streaming mode.</td>
</tr>
<tr>
<td>Last Interval (auto refresh)</td>
<td>- Select this option to filter your search results while in auto-refresh mode. The Log Activity and Network Activity tabs refreshes at one-minute intervals to display the most recent information.</td>
</tr>
<tr>
<td>Recent</td>
<td>- Select this option and, from this list box, select the time range that you want to filter for.</td>
</tr>
<tr>
<td>Specific Interval</td>
<td>- Select this option and, from the calendar, select the date and time range you want to filter for.</td>
</tr>
<tr>
<td>Include in my Quick Searches</td>
<td>Select this check box to include this search in your <a href="#">Quick Search</a> list box on the toolbar.</td>
</tr>
<tr>
<td>Include in my Dashboard</td>
<td>Select this check box to include the data from your saved search on the <a href="#">Dashboard</a> tab. For more information about the <a href="#">Dashboard</a> tab, see <a href="#">Dashboard management</a>.</td>
</tr>
<tr>
<td>Note:</td>
<td>This parameter is only displayed if the search is grouped.</td>
</tr>
<tr>
<td>Set as Default</td>
<td></td>
</tr>
<tr>
<td>Share with Everyone</td>
<td>Select this check box to share these search requirements with all users.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

**Deleting search criteria**

You can delete search criteria.

**About this task**

When you delete a saved search, then objects that are associated with the saved search might not function. Reports and anomaly detection rules are QRadar objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure that they continue to function.
Procedure
1. Click the Log Activity tab.
2. From the Search list box, select New Search or Edit Search.
3. In the Saved Searches pane, select a saved search from the Available Saved Searches list box.
4. Click Delete.
   • If the saved search criteria is not associated with other QRadar objects, a confirmation window is displayed.
   • If the saved search criteria is associated with other objects, the Delete Saved Search window is displayed. The window lists objects that are associated with the saved search that you want to delete. Note the associated objects.
5. Click OK.
6. Choose one of the following options:
   • Click OK to proceed.
   • Click Cancel to close the Delete Saved Search window.

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

Using a subsearch to refine search results
You can use a subsearch to search within a set of completed search results. The subsearch is used to refine search results, without searching the database again.

Before you begin
When you define a search that you want to use as a base for subsearching, make sure that Real Time (streaming) option is disabled and the search is not grouped.

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

Procedure
1. Click the Log Activity tab.
2. Perform a search.
3. When your search is complete, add another filter:
   a. Click Add Filter.
   b. From the first list box, select a parameter that you want to search for.
   c. From the second list box, select the modifier that you want to use for the search. The list of modifiers that are available depends on the attribute that is selected in the first list.
   d. In the entry field, type specific information that is related to your search.
   e. Click Add Filter.
**Results**

The Original Filter pane specifies the original filters that are applied to the base search. The Current Filter pane specifies the filters that are applied to the subsearch. You can clear subsearch 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 subsearch criteria, you still have access to saved subsearch criteria. If you add a filter, the subsearch searches the entire database since the search function no longer bases the search on a previously searched data set.

**What to do next**

- **Save search criteria**

---

**Managing search results**

You can initiate multiple 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**

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**

1. Click the **Log Activity** tab.
2. Perform a search.
3. Click **Save Results**.
4. On the Save Search Result window, type a unique name for the search results.
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 19. Manage search results page parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Indicates that an email notification is pending for when the search is complete.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies the name of the user who started the search.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the search, if the search has been saved. For more information about saving a search, see <a href="#">Saving search results</a>.</td>
</tr>
<tr>
<td>Started On</td>
<td>Specifies the date and time the search was started.</td>
</tr>
<tr>
<td>Ended On</td>
<td>Specifies the date and time the search ended.</td>
</tr>
<tr>
<td>Duration</td>
<td>Specifies the amount of time the search took to complete. If the search is in progress, the <strong>Duration</strong> parameter specifies how long the search has been processing to date. If the search was canceled, the <strong>Duration</strong> parameter specifies the period of time the search was processing before it was canceled.</td>
</tr>
<tr>
<td>Expires On</td>
<td>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 <a href="#">IBM Security QRadar Log Manager Administration Guide</a>.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status of the search. The statuses are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued</strong> - Specifies that the search is queued to start.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;percent&gt;%Complete</code> - Specifies the progress of the search in terms of percentage complete. You can click the link to view partial results.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sorting</strong> - Specifies that the search has finished collecting results and is currently preparing the results for viewing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Canceled</strong> - Specifies that the search has been canceled. You can click the link to view the results that were collected before the cancellation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Completed</strong> - Specifies that the search is complete. You can click the link to view the results. See <a href="#">Log activity monitoring</a>.</td>
</tr>
<tr>
<td>Size</td>
<td>Specifies the file size of the search result set.</td>
</tr>
</tbody>
</table>

The Manage Search Results window toolbar provides the following functions
Table 20. Manage Search Results toolbar

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Search</td>
<td>Click <strong>New Search</strong> to create a new search. When you click this icon, the search page is displayed.</td>
</tr>
<tr>
<td>Save Results</td>
<td>Click <strong>Save Results</strong> to save the selected search results. See Saving search results.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Click <strong>Cancel</strong> to cancel the selected search result that is in progress or are queued to start. See Canceling a search.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click <strong>Delete</strong> to delete the selected search result. See Deleting a search result.</td>
</tr>
<tr>
<td>Notify</td>
<td>Click <strong>Notify</strong> to enable email notification when the selected search is complete.</td>
</tr>
</tbody>
</table>
| 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
1. Click the **Log Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. View the list of search results.

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
1. Click the **Log Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. Select the queued or in progress search result you want to cancel.
4. Click **Cancel**.
5. Click **Yes**.

Deleting a search
If a search result is no longer required, you can delete the search result from the Manage Search Results page.
Procedure
1. Click the Log Activity tab.
2. From the Search menu, select Manage Search Results.
3. Select the search result that you want to delete.
4. Click Delete.
5. Click Yes.

Managing search groups

Using the Search Groups window, you can create and manage event, flow, and offense search groups.

These groups allow you to easily locate saved search criteria on the Log Activity tab and in the Report wizard.

Viewing search groups

A default set of groups and subgroups are available.

About this task

You can view search groups on the Event Search Group window.

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

The Event Search Group window displays the following parameters for each group.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the search group.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies the name of the user that created the search group.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description of the search group.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>Specifies the date the search group was modified.</td>
</tr>
</tbody>
</table>

The Event Search Group window toolbar provides the following functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Group</td>
<td>To create a new search group, you can click New Group. See Creating a new search group.</td>
</tr>
<tr>
<td>Edit</td>
<td>To edit an existing search group, you can click Edit. See Editing a search group.</td>
</tr>
<tr>
<td>Copy</td>
<td>To copy a saved search to another search group, you can click Copy. See Copying a saved search to another group.</td>
</tr>
</tbody>
</table>
Table 22. Search Group window toolbar functions (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>To remove a search group or a saved search from a search group, select the item that you want to remove, and then click <strong>Remove</strong>. See <a href="#">Removing a group or a saved search from a group</a>.</td>
</tr>
</tbody>
</table>

**Procedure**
1. Click the **Log Activity** tab.
2. Select **Search > Edit Search**.
3. Click **Manage Groups**.
4. View the search groups.

**Creating a new search group**
You can create a new search group.

**Procedure**
1. Click the **Log Activity** tab.
2. Select **Search > Edit Search**.
3. Click **Manage Groups**.
4. Select the folder for the group under which you want to create the new group.
5. Click **New Group**.
6. In the **Name** field, type a unique name for the new group.
7. Optional. In the **Description** field, type a description.
8. Click **OK**.

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

**Procedure**
1. Click the **Log Activity** tab.
2. Select **Search > Edit Search**.
3. Click **Manage Groups**.
4. Select the group that you want to edit.
5. Click **Edit**.
6. Edit the parameters:
   - Type a new name in the **Name** field.
   - Type a new description in the **Description** field.
7. Click **OK**.

**Copying a saved search to another group**
You can copy a saved search to one or more groups.

**Procedure**
1. Click the **Log Activity** tab.
2. Select **Search > Edit Search**.
3. Click Manage Groups.
4. Select the saved search that you want to copy.
5. Click Copy.
6. On the Item Groups window, select the check box for the group you want to copy the saved search to.
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 Event Search Groups from your system.

Procedure
1. Click the Log Activity tab.
2. Select Search > Edit Search.
3. Click Manage Groups.
4. Choose one of the following options:
   • Select the saved search that you want to remove from the group.
   • Select the group that you want to remove.
5. Click Remove.
6. Click OK.
Chapter 7. Custom event properties

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

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 that is 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 if you have the correct permission.

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 that you have the correct permissions.

For more information, see the IBM Security QRadar Log Manager Administration Guide.

Custom property types

You can create a custom property type.

When you create a custom property, you can choose to create a Regex or a calculated property type.

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

For example, a report is created to report all users who make user permission changes on an Oracle server. A list of users and the number of times they made a change to the permission of another account is reported. However, typically the actual user account or permission that was changed cannot display. 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.

Using calculation-based custom properties, you can perform calculations on existing numeric event or flow 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.

### Creating a regex-based custom property

You can create a regex-based custom property to match event or flow payloads to a regular expression.

**About this task**

When you configure a regex-based custom property, the Custom Event Property window provides parameters. The following table describes some of these parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test field</td>
<td>Specifies the payload that was extracted from the unnormalized event or flow.</td>
</tr>
<tr>
<td></td>
<td>Specifies the payload that was extracted from the unnormalized event.</td>
</tr>
<tr>
<td>New Property</td>
<td>The new property name cannot be the name of a normalized property, such as username, Source IP, or Destination IP.</td>
</tr>
<tr>
<td>Optimize parsing for rules, reports, and searches</td>
<td>Parses and stores the property the first time that the event or flow is received. When you select the check box, the property does not require more parsing for reporting, searching, or rule testing.</td>
</tr>
<tr>
<td></td>
<td>If you clear this check box, the property is parsed each time a report, search, or rule test is applied.</td>
</tr>
<tr>
<td>Log Source</td>
<td>If multiple log sources are associated with this event, this field specifies the term Multiple and the number of log sources.</td>
</tr>
</tbody>
</table>
Table 23. Custom Event Properties window parameters (regex) (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| RegEx     | The regular expression that you want to use for extracting the data from the payload. Regular expressions are case-sensitive. The following examples show sample regular expressions:  
  - Email: (\+@[^\s]+\.[a-z]+)$  
  - URL: (http://[a-zA-Z0-9-\.]+\.[a-zA-Z]{2,3}\/[\w\\s]*)?$  
  - Domain Name: (http[s]?://([^\//]+)\/?)  
  - Floating Point Number: \([-+]?\d*\d*$  
  - Integer: \([-+]?\d*\d*$  
  - IP address: (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})|
| Capture Group | Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses. |
| Enabled   | 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. |

**Procedure**

1. Click the **Log Activity** tab.
2. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event that you want to base the custom property on.
4. Click **Extract Property**.
5. In the **Property Type Selection** pane, select the **Regex Based** option.
6. Configure the custom property parameters.
7. Click **Test** to test the regular expression against the payload.
8. Click **Save**.

**Results**

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

**Creating a calculation-based custom property**

You can create a calculation-based customer property to match payloads to a regular expression.
About this task

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

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

Procedure

1. Choose one of the following: Click the Log Activity tab.
2. Optional. If you are viewing events or flows in streaming mode, click the Pause icon to pause streaming.
3. Double-click the event you want to base the custom property on.
4. Click Extract Property.
5. In the Property Type Selection pane, select the Calculation Based option.
6. Configure the custom property parameters.
7. Click Test to test the regular expression against the payload.
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 or flows list, you must select the custom property from the list of available columns when creating a search.

---

**Modifying a custom property**

You can modify a custom property.

**About this task**

You can use the Custom Event Properties window to modify a custom property.

The custom properties are described in the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Name</td>
<td>Specifies a unique name for this custom property.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type for this custom property.</td>
</tr>
<tr>
<td>Property Description</td>
<td>Specifies a description for this custom property.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>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.</td>
</tr>
<tr>
<td>Log Source</td>
<td>Specifies the log source to which this custom property applies.</td>
</tr>
<tr>
<td></td>
<td>If there are multiple log sources that are 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.</td>
</tr>
</tbody>
</table>
Table 25. Custom properties window columns (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression</td>
<td>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 that you want to use for extracting the data from the payload. For a calculation-based custom property, this parameter specifies the calculation that you want to use to create the custom property value.</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the name of the user who created this custom property.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Specifies whether this custom property is enabled. This field specifies either True or False.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Specifies the date this custom property was created.</td>
</tr>
<tr>
<td>Modification Date</td>
<td>Specifies the last time this custom property was modified.</td>
</tr>
</tbody>
</table>

The Custom Event Property toolbar provides the following functions:

Table 26. Custom property toolbar options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click Add to add a new custom property.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click Edit to edit the selected custom property.</td>
</tr>
<tr>
<td>Copy</td>
<td>Click Copy to copy selected custom properties.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click Delete to delete selected custom properties.</td>
</tr>
<tr>
<td>Enable/Disable</td>
<td>Click Enable/Disable to enable or disable the selected custom properties for parsing and viewing in the search filters or column lists.</td>
</tr>
</tbody>
</table>

Procedure
1. Click the Log Activity tab.
2. From the Search list box, select Edit Search.
3. Click Manage Custom Properties.
4. Select the custom property that you want to edit and click Edit.
5. Edit the necessary parameters.
6. Optional. If you edited the regular expression, click Test to test the regular expression against the payload.
7. Click Save.
Copying a custom property

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

Procedure
1. Click the Log Activity tab.
2. From the Search list box, select Edit Search.
3. Click Manage Custom Properties.
4. Select the custom property that you want to copy and click Copy.
5. Edit the necessary parameters.
6. Optional. If you edited the regular expression, click Test to test the regular expression against the payload.
7. Click Save.

Deleting a custom property

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

Procedure
1. From the Search list box, select Edit Search.
2. Click Manage Custom Properties.
3. Select the custom property that you want to delete and click Delete.
4. Click Yes.
Chapter 8. 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 you have the View Custom Rules and Maintain Custom Rules user role permissions.

To create anomaly detection rules, you must have the appropriate Maintain Custom Rule permission for the tab on which you want to create the rule. For example, to be able to create an anomaly detection rule on the Log Activity tab, you must have the Log Activity > Maintain Custom Rule.

For more information about user role permissions, see the IBM Security QRadar Log Manager Administration Guide.

Rules overview

Rules perform tests on events and if all the conditions of a test are met, the rule generates a response.

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.

For a complete list of default rules, see the IBM Security QRadar SIEM Administration Guide.

Event rule

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. It is common for event rules to create offenses as a response.

Rule conditions

Each rule might contain functions, building blocks, or tests.

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 when an event matches any/all of the following rules function.
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 will allow you to reuse 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.

You can run tests on the property of an event such as source IP address or severity of event.

Rule responses

When rule conditions are met, a rule can generate one or more responses.

Rules can generate one or more of the following responses:

- Create an offense.
- Send an email.
- Generate system notifications on the Dashboard feature.
- Add data to reference sets.
- Add data to reference data collections.
- Generate a response to an external system.
- Add data to reference data collections that can be used in rule tests.

Reference data collection types

Before you can configure a rule response to send data to a reference data collection, you must create the reference data collection by using the command line interface (CLI). QRadar supports the following data collection types:

Reference set
A set of elements, such as a list of IP addresses or user names, that are derived from events and flows occurring on your network.

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
Data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, use a custom event property for Patent ID as the key and the Username parameter as the value. Use a map of sets to populate a list of authorized users.

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. Use the Source IP parameter as the first key, the Application parameter as the second key, and the Total Bytes parameter as the value.

Reference table
In a reference table, data is stored in a table that maps one key to another key, which is then mapped to single value. The second key has an assigned
type. This mapping is similar to a database table where each column in the table is associated with a type. For example, you can create a reference table that stores the Username parameter as the first key, and has multiple secondary keys that have a user-defined assigned type such as IP Type with the Source IP or Source Port parameter as a value. You can configure a rule response to add one or more keys defined in the table. You can also add custom values to the rule response. The custom value must be valid for the secondary key’s type.

Note: For information about reference sets and reference data collections, see the Administration Guide for your product.

### 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 Log Activity tab. For more information about 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. 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.

**Procedure**

1. Click the Log Activity tab, and then select Rules from the Rules list box on the toolbar.
2. From the Display list box, select Rules.
3. Double-click the rule that you want to view.
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.

### Creating a custom rule

You can create new rules to meet the needs of your deployment.

**About this task**

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

You can test rules locally or globally. A local test means that rule is tested on the local Event processor and not shared with the system. A global test means that the rule is shared and tested by any Event processor on the system. Global rules send
events and flows to the central Event processor, which might decrease performance on the central Event processor.

**Procedure**

1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. From the Actions list, select New Event Rule.
4. Read the introductory text on the Rule wizard. Click Next.
5. Click Next to view the Rule Test Stack Editor page.
6. In the enter rule name here field in the Rule pane, type a unique name that you want to assign to this rule.
7. From the list box, select Local or Global.
8. Add one or more tests to a rule:
   a. Optional. To filter the options in the Test Group list box, type the text that 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 plus (+) 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.
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.
10. On the Groups pane, select the check boxes of the groups to which you want to assign this rule.
11. In the Notes field, type a note that you want to include for this rule. Click Next.
12. On the Rule Responses page, configure the responses that you want this rule to generate.
13. Click Next.
14. Review the Rule Summary page to ensure that the settings are correct. Make changes if necessary, and then click Finish.

### Creating an anomaly detection rule

Use the Anomaly Detection Rule wizard to create rules that apply time range criteria by using Data and Time tests.

**Before you begin**

To create a new anomaly detection rule, you must meet the following requirements:

- Have the Maintain Custom Rules permission.
- Perform a grouped search.
The anomaly detection options display after you perform a grouped search and save the search criteria.

**About this task**

You must have the appropriate role permission to be able to create an anomaly detection rule.

To create anomaly detection rules on the **Log Activity** tab, you must have the **Log Activity Maintain Custom Rules** role permission.

To create anomaly detection rules on the **Network Activity** tab, you must have the **Network Maintain Custom Rules** role permission.

Anomaly detection rules use all grouping and filter criteria from the saved search criteria the rule is based on, but do not use any time ranges from the search criteria.

When you create an anomaly detection rule, the rule is populated with a default test stack. You can edit the default tests or add tests to the test stack. At least one Accumulated Property test must be included in the test stack.

By default, the **Test the [Selected Accumulated Property] value of each [group] separately** option is selected on the Rule Test Stack Editor page.

This causes an anomaly detection rule to test the selected accumulated property for each event group separately. For example, if the selected accumulated value is **UniqueCount(sourceIP)**, the rule tests each unique source IP address for each event group.

This **Test the [Selected Accumulated Property] value of each [group] separately** option is dynamic. The **[Selected Accumulated Property]** value depends on what option you select for the **this accumulated property test** field of the default test stack. The **[group]** value depends on the grouping options that are specified in the saved search criteria. If multiple grouping options are included, the text might be truncated. Move your mouse pointer over the text to view all groups.

**Procedure**

1. Click the **Log Activity** tab.
2. Perform a search.
3. From the **Rules** menu, select the rule type that you want to create. Options include:
   - Add Anomaly Rule
   - Add Threshold Rule
   - Add Behavioral Rule
4. Read the introductory text on the Rule wizard. Click **Next**. The rule that you previously choose is selected.
5. Click **Next** to view the Rule Test Stack Editor page.
6. In the **enter rule name here** field, type a unique name that you want to assign to this rule.
7. To add a test to a rule:
   a. Optional. To filter the options in the Test Group list box, type the text that 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.

8. Optional. To test the total selected accumulated properties for each event or flow group, clear the Test the [Selected Accumulated Property] value of each [group] separately check box.

9. In the groups pane, select the check boxes of the groups you want to assign this rule to. For more information, see Rule group management.

10. In the Notes field, type any notes that you want to include for this rule. Click Next.

11. On the Rule Responses page, configure the responses that you want this rule to generate. “Rule Response page parameters” on page 85

12. Click Next.

13. Review the configured rule. Click Finish.

Rule management tasks

You can manage custom and anomaly rules.

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

You can create anomaly detection rules only on the Log Activity tab.

Enabling and disabling rules

When you tune your system, you can enable or disable the appropriate rules to ensure that your system generates meaningful offenses 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

1. Click the Log Activity tab.

2. On the toolbar, click Rules.

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

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

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 enable or disable a rule.

Procedure
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. From the Display list box on the Rules page, select Rules.
4. Double-click the rule that you want to edit.
5. From the Actions list box, select Open.
6. Optional. If you want to change the rule type, click Back and select a new rule type.
7. On the Rule Test Stack Editor page, edit the parameters.
8. Click Next.
10. Click Next.
11. Review the edited rule. Click Finish.

Copying a 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 enable or disable a rule.

Procedure
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. From the Display list box, select Rules.
4. Select the rule that you want to duplicate.
5. From the Actions list box, select Duplicate.
6. In the Enter name for the copied rule field, type a name for the new rule. Click OK.

Deleting a rule
You can delete a rule from your system.

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

Procedure
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. From the Display list box, select Rules.
4. Select the rule that you want to delete.
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 that are related to compliance.

As you create new rules, you can assign the rule to an existing group. For information about assigning a group using the rule wizard, see [Creating a custom rule](#) or [Creating an anomaly detection 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 that belong to a specific group.

**Procedure**

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules**.
3. From the **Display** list box, select whether you want to view rules or building blocks.
4. From the **Filter** list box, select the group category that you want to view.

**Creating a group**

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

**Procedure**

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules**.
3. Click **Groups**.
4. From the navigation tree, select the group under which you want to create a new group.
5. Click **New Group**.
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 that you want to assign to this group. The description can be up to 255 characters in length.
7. Click **OK**.
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.

**Assigning an item to a group**

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

1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. Select the rule or building block you want to assign to a group.
4. From the Actions list box, select Assign Groups.
5. Select the group that you want to assign the rule or building block to.
6. Click Assign Groups.
7. Close the Choose Groups window.

**Editing a group**

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

**Procedure**

1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. Click Groups.
4. From the navigation tree, select the group that you want to edit.
5. Click Edit.
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 that you want to assign to this group. The description can be up to 255 characters in length.
7. Click OK.
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.

**Copying an item to another group**

You can copy a rule or building block from one group to other groups.

**Procedure**

1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. Click Groups.
4. From the navigation tree, select the rule or building block you want to copy to another group.
5. Click Copy.
6. Select the check box for the group you want to copy the rule or building block to.
7. Click Copy.

**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**
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. Click Groups.
4. Using the navigation tree, navigate to and select the item you want to delete.
5. Click Remove.
6. Click OK.

**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**
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. Click Groups.
4. Using the navigation tree, navigate to and select the group that you want to delete.
5. Click Remove.
6. Click OK.

**Editing building blocks**
You can edit any of the default building blocks to match the needs of your deployment.

**About this task**
A building block is a reusable 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.

**Procedure**
1. Click the Log Activity tab.
2. On the toolbar, click Rules.
3. From the Display list box, select Building Blocks.
4. Double-click the building block that you want to edit.
5. Update the building block, as necessary.
6. Click Next.
7. Continue through the wizard. For more information, see Creating a custom rule.
8. Click Finish.
## Rule page parameters

A description of the parameters on the Rules page.

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

Table 27. Rules page parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Displays the name of the rule.</td>
</tr>
<tr>
<td>Group</td>
<td>Displays the group to which this rule is assigned. For more information about groups, see Rule group management.</td>
</tr>
<tr>
<td>Rule Category</td>
<td>Displays the rule category for the rule. Options include Custom Rule and Anomaly Detection Rule.</td>
</tr>
<tr>
<td>Rule Type</td>
<td>Displays the rule type.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the rule is enabled or disabled. For more information about enabling and disabling rules, see Enabling and disabling rules.</td>
</tr>
<tr>
<td>Event Count</td>
<td>Displays the number of events that are associated with this rule when the rule contributes to an offense.</td>
</tr>
<tr>
<td>Origin</td>
<td>Displays whether this rule is a default rule (System) or a custom rule (User).</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Specifies the date and time this rule was created.</td>
</tr>
<tr>
<td>Modification Date</td>
<td>Specifies the date and time this rule was modified.</td>
</tr>
</tbody>
</table>
## Rules page toolbar

You use the Rules page toolbar to display rules, building blocks or groups. You can manage rule groups and work with rules.

The Rules page toolbar provides the following functions:

**Table 28. Rules page toolbar function**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>From the list box, select whether you want to display rules or building blocks in the rules list.</td>
</tr>
<tr>
<td>Group</td>
<td>From the list box, select which rule group you want to be displayed in the rules list.</td>
</tr>
<tr>
<td>Groups</td>
<td>Click <strong>Groups</strong> to manage rule groups.</td>
</tr>
<tr>
<td>Actions</td>
<td>Click <strong>Actions</strong> and select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>New Event Rule</strong> - Select this option to create a new event rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable/Disable</strong> - Select this option to enable or disable selected rules.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Duplicate</strong> - Select this option to copy a selected rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> - Select this option to edit a selected rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete</strong> - Select this option to delete a selected rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assign Groups</strong> - Select this option to assign selected rules to rule groups.</td>
</tr>
<tr>
<td>Revert Rule</td>
<td>Click <strong>Revert Rule</strong> to revert a modified system rule to the default value. When you click <strong>Revert Rule</strong>, a confirmation window is displayed. When you revert a rule, any previous modifications are permanently removed.</td>
</tr>
</tbody>
</table>

To revert the rule and maintain a modified version, duplicate the rule and use the **Revert Rule** option on the modified rule.
Table 28. Rules page toolbar function (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**

There are parameters for the Rule Response page.

The following table provides the Rule Response page parameters.

Table 29. Event, Flow, and Common Rule Response page parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>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.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
<tr>
<td>Relevance</td>
<td>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.</td>
</tr>
<tr>
<td>Annotate event</td>
<td>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.</td>
</tr>
<tr>
<td>Drop the detected event</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Dispatch New Event   | Select this check box to dispatch a new event in addition to the original event, which is 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.                                     |
### Table 29. Event, Flow, and Common Rule Response page parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>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.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
<tr>
<td>Relevance</td>
<td>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 Annotation pane of the event details.</td>
</tr>
<tr>
<td>High-Level Category</td>
<td>From the list box, select the high-level event category that you want this rule to use when processing events.</td>
</tr>
<tr>
<td>Low-Level Category</td>
<td>From the list box, select the low-level event category that you want this rule to use when processing events.</td>
</tr>
<tr>
<td>Email</td>
<td>Select this check box to display the email options. By default, the check box is clear.</td>
</tr>
<tr>
<td>Enter email addresses to notify</td>
<td>Type the email address to send notification if this rule generates. Use a comma to separate multiple email addresses.</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. 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 MIB.</td>
</tr>
<tr>
<td>Send to Local SysLog</td>
<td>Select this check box if you want to log the event locally. By default, this check box is clear.</td>
</tr>
<tr>
<td>Send to Forwarding Destinations</td>
<td>This check box is only displayed for Event rules. Select this check box if you want to log the event or flow 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 or flow to. To add, edit, or delete a forwarding destination, click the Manage Destinations link.</td>
</tr>
<tr>
<td>Notify</td>
<td>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. If you enable notifications, configure the Response Limiter parameter.</td>
</tr>
</tbody>
</table>
Table 29. Event, Flow, and Common Rule Response page parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Reference Set</td>
<td>Select this check box if you want events that are generated as a result of this rule to add data to a reference set.</td>
</tr>
<tr>
<td></td>
<td>To add data to a reference set:</td>
</tr>
<tr>
<td></td>
<td>1. Using the first list box, select the data that you want to add. Options include all normalized or custom data.</td>
</tr>
<tr>
<td></td>
<td>2. Using the second list box, select the reference that is set to which you want to add the specified data.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Add to Reference Set</strong> rule response provides the following functions:</td>
</tr>
<tr>
<td>Refresh</td>
<td>Click <strong>Refresh</strong> to refresh the first list box to ensure that the list is current.</td>
</tr>
<tr>
<td>Configure Reference Sets</td>
<td>Click <strong>Configure Reference Sets</strong> to configure the reference set. This option is only available if you have administrative permissions.</td>
</tr>
</tbody>
</table>
Table 29. Event, Flow, and Common Rule Response page parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add to Reference Data    | Before you can use this rule response, you must create the reference data collection by using the command line interface (CLI). For more information about how to create and use reference data collections, see the Administration Guide for your product. Select this check box if you want events that are 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 that 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.  
  **Add to a Reference Table**  
  Select this option to send data to a collection of multiple key/single value pairs, where a type was assigned to the secondary keys. Select the reference table that you want to add data to, and then select a primary key. Select your inner keys (secondary keys) and their values for the data records. |
| 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 about the IF-MAP server. |
| 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. |

An SNMP notification might resemble:

"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -  
Rule 'SNMPTRAPtst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 i, Event Name:  
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes:  
Offense description"

A 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
Chapter 9. Asset profiles

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, then QRadar 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.

About vulnerabilities

You can use QRadar Vulnerability Manager and third-party scanners to identify vulnerabilities.

Third-party scanners identify and report discovered vulnerabilities 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. The OSVDB assigns a unique reference identifier (OSVDB ID) to each vulnerability. 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 Manager User Guide.

QRadar Vulnerability Manager is a 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 rerun 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 scans on selected assets.

For more information, see the IBM Security QRadar Vulnerability Manager User 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.
• Configure and manage third-party vulnerability scanning.
• Start QRadar Vulnerability Manager scans.

For more information about the VA Scan option in the navigation pane, see the IBM Security QRadar Risk Manager User Guide.

Asset tab list

The Asset Profiles page provides information about ID, IP address, Asset name, Aggregate CVSS score, Vulnerabilities, and Services.

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

Table 30. Asset Profile page parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Displays the Asset ID number of the asset. The Asset ID number is automatically generated when you add an asset profile manually or when assets are discovered by event or vulnerability scans.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the last known IP address of the asset.</td>
</tr>
<tr>
<td>Asset Name</td>
<td>Displays the given name, NetBios name, DSN name, or MAC address of the asset. If unknown, this field displays the last known IP address.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If the asset is automatically discovered, this field is automatically populated, however, you can edit the asset name if required.</td>
</tr>
</tbody>
</table>
### Table 30. Asset Profile page parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Score</td>
<td>Displays the one of the following Common Vulnerability Scoring System (CVSS) scores:</td>
</tr>
<tr>
<td></td>
<td>• Coalesced aggregate environmental CVSS score</td>
</tr>
<tr>
<td></td>
<td>• Aggregate temporal CVSS score</td>
</tr>
<tr>
<td></td>
<td>• Aggregate CVSS base score</td>
</tr>
</tbody>
</table>

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 from 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" on page 97.

For more information about CVSS, see [http://www.first.org/cvss/](http://www.first.org/cvss/).

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Displays the number of unique vulnerabilities that are discovered on this asset. This value also includes the number of active and passive vulnerabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Displays the number of unique Layer 7 applications that run on this asset.</td>
</tr>
<tr>
<td>Last User</td>
<td>Displays the last user associated with the asset.</td>
</tr>
<tr>
<td>User Last Seen</td>
<td>Displays the time when the last user associated with the asset was last seen.</td>
</tr>
</tbody>
</table>

**Assets tab toolbar**

The Asset Profiles page toolbar allows you to search, save, add, clear, edit, and perform other actions on assets.

The Asset Profiles page toolbar provides the following functions:
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Click <strong>Search</strong> 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 <a href="#">Searching asset profiles</a>.</td>
</tr>
<tr>
<td>Quick Searches</td>
<td>From this list box, you can run previously saved searches. Options are displayed in the <strong>Quick Searches</strong> list box only when you have saved search criteria that specifies the <strong>Include in my Quick Searches</strong> option.</td>
</tr>
<tr>
<td>Save Criteria</td>
<td>Click <strong>Save Criteria</strong> to save the current search criteria.</td>
</tr>
<tr>
<td>Add Filter</td>
<td>Click <strong>Add Filter</strong> to add a filter to the current search results.</td>
</tr>
<tr>
<td>Add Asset</td>
<td>Click <strong>Add Asset</strong> to add an asset profile. See <a href="#">Adding or editing an asset profile</a>.</td>
</tr>
<tr>
<td>Edit Asset</td>
<td>Click <strong>Edit Asset</strong> 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” on page 97.</td>
</tr>
<tr>
<td>Actions</td>
<td>Click <strong>Actions</strong> to perform the following actions: * Delete Asset - Select this option to delete the selected asset profiles. See <a href="#">Deleting assets</a> * Delete Listed - Select this option to delete all asset profiles that are listed in the results list. See <a href="#">Deleting assets</a> * Import Assets - Select this option to import assets. See <a href="#">Importing asset profiles</a> * Export to XML - Select this option to export asset profiles in XML format. See <a href="#">Exporting assets</a> * Export to CSV - Select this option to export asset profiles in CSV format. See <a href="#">Exporting assets</a> * Print - Select this option to print the asset profiles that are displayed on the page.</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>After you apply a filter using the <strong>Add Filter</strong> option, you can click <strong>Clear Filter</strong> to remove the filter.</td>
</tr>
</tbody>
</table>
Right-click menu options

Right-clicking an asset on the Asset tab displays Navigate, Information, and Run QVM Scan menus for more event filter information.

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

Table 32. Right-click menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>The Information menu provides the following options:</td>
</tr>
<tr>
<td></td>
<td>- DNS Lookup - Searches for DNS entries that are based on the IP address.</td>
</tr>
<tr>
<td></td>
<td>- WHOIS Lookup - Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- Asset Profile - Displays asset profile information. This menu option is only available when asset profile data is acquired actively by a scan.</td>
</tr>
<tr>
<td></td>
<td>- Search Events - Select the Search Events option to search events that are associated with this IP address.</td>
</tr>
<tr>
<td>Run QVM Scan</td>
<td>Select this option to run a Vulnerability Manager scan on the selected asset.</td>
</tr>
<tr>
<td></td>
<td>This option is displayed only after you install QRadar Vulnerability Manager.</td>
</tr>
</tbody>
</table>

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 about each profile.

About this task

Asset profile information is automatically discovered through Server Discovery or manually configured. You can edit automatically generated asset profile information.

The Asset Profile page provides the information about the asset that is 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.

The Asset Profile page toolbar provides the following functions:
<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to Asset List</td>
<td>Click this option to return to the asset list.</td>
</tr>
<tr>
<td>Display</td>
<td>From the list box, you can select the pane that you want to view on the Asset Profile pane. The Asset Summary and Network Interface Summary panes are always displayed.</td>
</tr>
<tr>
<td></td>
<td>For more information about the parameters that are displayed in each pane, see <a href="#">Assets profile page</a>.</td>
</tr>
<tr>
<td>Edit Asset</td>
<td>Click this option to edit the Asset Profile. See “Adding or editing an asset profile” on page 97.</td>
</tr>
<tr>
<td>View Destination Summary</td>
<td>If this asset is the destination of an offense, this option will allow you to view destination summary information.</td>
</tr>
<tr>
<td>History</td>
<td>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 event search criteria:</td>
</tr>
<tr>
<td></td>
<td>You can customize the search parameters, if required. Click Search to view the event history information.</td>
</tr>
<tr>
<td>Applications</td>
<td>Click Applications to view application information for this asset. When you click the Applications icon, the Flow Search window is displayed, pre-populated with event search criteria.</td>
</tr>
<tr>
<td></td>
<td>You can customize the search parameters, if required. Click Search to view the application information.</td>
</tr>
<tr>
<td>Search Connections</td>
<td>Click Search Connections to search for connections. The Connection Search window is displayed.</td>
</tr>
<tr>
<td></td>
<td>This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager User Guide.</td>
</tr>
<tr>
<td>View Topology</td>
<td>This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager User Guide.</td>
</tr>
<tr>
<td>Actions</td>
<td>From the Actions list, select Vulnerability History.</td>
</tr>
<tr>
<td></td>
<td>This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager User Guide.</td>
</tr>
</tbody>
</table>
Procedure
1. Click the Assets tab.
2. On the navigation menu, click Asset Profiles.
3. Double-click the asset that you want to view.
4. Use the options on the toolbar to display the various panes of asset profile information. See Editing an asset profile.
5. To research the associated vulnerabilities, click each vulnerability in the Vulnerabilities pane. See Table 10-10.
6. If required, edit the asset profile. See Editing an asset profile.
7. Click Return to Assets List to select and view another asset, if required.

Adding or editing an asset profile

Asset profiles are automatically discovered and added; however, you might be required to manually add a profile.

About this task

When assets are discovered 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.

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
1. Click the Assets tab.
2. On the navigation menu, click Asset Profiles.
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 that you want to view and click Edit Asset.
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.
5. Configure the parameters in the Names & Description pane. Configure one or more of the following options:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**. |
| 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. |

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.  

7. Configure the parameters in the CVSS & Weight pane. Configure one or more of the following options:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 - 10. When you configure the Weight parameter, the Collateral Damage Potential parameter is automatically updated. |
Searching asset profiles

You can configure search parameters to display only the asset profiles you want to investigate from the Asset page on the Assets tab.

About this task

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.

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

The search feature will allow you to search host profiles, assets, and identity information. Identity information provides more detail 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 whether known vulnerabilities exist in your deployment.

For example:

You receive a notification that CVE ID: CVE-2010-000 is being actively used in the field. To verify whether 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

1. Click the Assets tab.
2. On the navigation menu, click Asset Profiles.
3. On the toolbar, click Search > New Search.
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.
5. Select a previously saved search:
   a. Choose one of the following options:
      • Optional. From the Group list box, select the asset search group that you want to display in the Available Saved Searches list.
      • From the Available Saved Searches list, select the saved search that 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.
6. In the Search Parameters pane, define your search criteria:
a. From the first list box, select the asset parameter that you want to search for. For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.

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

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

d. Click **Add Filter**.

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

7. Click **Search**.

**Results**

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 reuse the criteria. Saved search criteria does not expire.

**Procedure**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Perform a search. See [Searching asset profiles](#).
4. Click **Save Criteria**.
5. Enter values for the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the name of this search</td>
<td>Type the unique name that you want to assign to this search criteria.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>Click <strong>Manage Groups</strong> to manage search groups. For more information, see <a href="#">Asset search groups</a>. This option is only displayed if you have administrative permissions.</td>
</tr>
<tr>
<td>Assign Search to Group(s)</td>
<td>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 <a href="#">Asset search groups</a>.</td>
</tr>
<tr>
<td>Include in my Quick Searches</td>
<td>Select this check box to include this search in your <strong>Quick Search</strong> list box, which is on the <strong>Assets</strong> tab toolbar.</td>
</tr>
<tr>
<td>Set as Default</td>
<td>Select this check box to set this search as your default search when you access the <strong>Assets</strong> tab.</td>
</tr>
<tr>
<td>Share with Everyone</td>
<td>Select this check box to share these search requirements with all users.</td>
</tr>
</tbody>
</table>
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 tab.

Viewing search groups

Use the Asset Search Groups window to view a list group and subgroups.

About this task

From the Asset Search Groups window, you can view details about each group, including a description and the date the group was last modified.

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

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Group</td>
<td>To create a new search group, you can click New Group. See See Creating a new search group.</td>
</tr>
<tr>
<td>Edit</td>
<td>To edit an existing search group, you can click Edit. See See Editing a search group.</td>
</tr>
<tr>
<td>Copy</td>
<td>To copy a saved search to another search group, you can click Copy. See See Copying a saved search to another group.</td>
</tr>
<tr>
<td>Remove</td>
<td>To remove a search group or a saved search from a search group, select the item that you want to remove, and then click Remove. See See Removing a group or a saved search from a group.</td>
</tr>
</tbody>
</table>

Procedure

1. Click the Assets tab.
2. On the navigation menu, click Asset Profiles.
4. Click on Manage Groups.
5. View the search groups.

Creating a new search group

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

Procedure

1. Click the Assets tab.
2. On the navigation menu, click Asset Profiles.
4. Click Manage Groups.
5. Select the folder for the group under which you want to create the new group.
6. Click **New Group**.
7. In the **Name** field, type a unique name for the new group.
8. Optional. In the **Description** field, type a description.
9. Click **OK**.

### Editing a search group

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

**Procedure**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search > New Search**.
4. Click **Manage Groups**.
5. Select the group that you want to edit.
6. Click **Edit**.
7. Type a new name in the **Name** field.
8. Type a new description in the **Description** field.
9. 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**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search > New Search**.
4. Click **Manage Groups**.
5. Select the saved search that you want to copy.
6. Click **Copy**.
7. On the Item Groups window, select the check box for the group you want to copy the saved search to.
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**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
4. Click **Manage Groups**.
5. Select the saved search that you want to remove from the group:
   - Select the saved search that you want to remove from the group.
   - Select the group that you want to remove.

---

**Asset profile management tasks**

You can delete, import, and export asset profiles using the Assets tab.

**About this task**

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**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select the asset that you want to delete, and then select **Delete Asset** from the **Actions** list box.
4. Click **OK**.

**Importing asset profiles**

You can import asset profile information.

**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**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. From the **Actions** list box, select **Import Assets**.
4. Click **Browse** to locate and select the CSV file that you want to import.
5. Click **Import Assets** to begin the import process.

**Exporting assets**

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

**Procedure**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. From the **Actions** list box, select one of the following options:
   - Export to XML
   - Export to CSV
4. View the status window for the status of the export process.
5. Optional: If you want to use other tabs and pages while the export is in progress, click the **Notify When Done** link.
   
   When the export is complete, the File Download window is displayed.
6. 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.
7. Click **OK**.

**Research asset vulnerabilities**

The Vulnerabilities pane on the Asset Profile page displays a list of discovered vulnerabilities for the asset.

**About this task**

You can double-click the vulnerability to display more vulnerability details.

The Research Vulnerability Details window provides the following details:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability ID</td>
<td>Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Published Date</td>
<td>Specifies the date on which the vulnerability details were published on the OSVDB.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the vulnerability.</td>
</tr>
<tr>
<td>Assets</td>
<td>Specifies the number of assets in your network that have this vulnerability. Click the link to view the list of assets.</td>
</tr>
<tr>
<td>Assets, including exceptions</td>
<td>Specifies the number of assets in your network that have vulnerability exceptions. Click the link to view the list of assets.</td>
</tr>
<tr>
<td>CVE</td>
<td>Specifies the CVE identifier for the vulnerability. CVE identifiers are provided by the NVDB.</td>
</tr>
<tr>
<td></td>
<td>Click the link to obtain more information. When you click the link, the NVDB website is displayed in a new browser window.</td>
</tr>
<tr>
<td>xforce</td>
<td>Specifies the X-Force identifier for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>OSVDB</td>
<td>Specifies the OSVDB identifier for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>Click the link to obtain more information. When you click the link, the OSVDB website is displayed in a new browser window.</td>
</tr>
<tr>
<td>CVSS Score</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The CVSS score is calculated using the following user-defined parameters:</td>
</tr>
<tr>
<td></td>
<td>• Collateral Damage Potential</td>
</tr>
<tr>
<td></td>
<td>• Confidentiality Requirement</td>
</tr>
<tr>
<td></td>
<td>• Availability Requirement</td>
</tr>
<tr>
<td></td>
<td>• Integrity Requirement</td>
</tr>
<tr>
<td></td>
<td>For more information about how to configure these parameters, see “Adding or editing an asset profile” on page 97.</td>
</tr>
<tr>
<td></td>
<td>For more information about CVSS, see <a href="http://www.first.org/cvss">http://www.first.org/cvss</a>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Impact</td>
<td>Displays the type of harm or damage that can be expected if this vulnerability is exploited.</td>
</tr>
<tr>
<td>CVSS Base Metrics</td>
<td>Displays the metrics that are used to calculate the CVSS base score, including:</td>
</tr>
<tr>
<td></td>
<td>• Access Vector</td>
</tr>
<tr>
<td></td>
<td>• Access complexity</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Confidentiality impact</td>
</tr>
<tr>
<td></td>
<td>• Integrity impact</td>
</tr>
<tr>
<td></td>
<td>• Availability impact</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.</td>
</tr>
<tr>
<td>Concern</td>
<td>Specifies the effects that the vulnerability can have on your network.</td>
</tr>
<tr>
<td>Solution</td>
<td>Follow the instructions that are provided to resolve the vulnerability.</td>
</tr>
<tr>
<td>Virtual Patching</td>
<td>Displays virtual patch information that is 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.</td>
</tr>
<tr>
<td>Reference</td>
<td>Displays a list of external references, including:</td>
</tr>
<tr>
<td></td>
<td>• Reference Type - Specifies the type of reference that is listed, such as an advisory URL or mail post list.</td>
</tr>
<tr>
<td></td>
<td>• URL - Specifies the URL that you can click to view the reference.</td>
</tr>
<tr>
<td></td>
<td>Click the link to obtain more information. When you click the link, the external resource is displayed in a new browser window.</td>
</tr>
<tr>
<td>Products</td>
<td>Displays a list of products that are associated with this vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• Vendor - Specifies the vendor of the product.</td>
</tr>
<tr>
<td></td>
<td>• Product - Specifies the product name.</td>
</tr>
<tr>
<td></td>
<td>• Version - Specifies the version number of the product.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select an asset profile.
4. In the Vulnerabilities pane, click the **ID** or **Vulnerability** parameter value for the vulnerability you want to investigate.

**Assets profile page parameters**

You can find Asset profile page parameter descriptions for the Asset Summary pane, Network Interface pane, Vulnerability pane, Services pane, Packages pane, Windows Patches pane, Properties pane, Risk Policies pane, and Products pane.

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

**Asset Summary pane**

You can find parameter descriptions for the Asset Summary pane that you access from the Asset Profile page.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset ID</strong></td>
<td>Displays the ID number that is assigned to the asset profile.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the last reported IP address of the asset.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>Displays the last known MAC address of the asset.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Displays the last reported network that is associated with the asset.</td>
</tr>
<tr>
<td><strong>NetBIOS Name</strong></td>
<td>Displays the NetBIOS name of the asset, if known. If the asset has more than</td>
</tr>
<tr>
<td></td>
<td>one NetBIOS name, this field indicates the number of NetBIOS names. Move</td>
</tr>
<tr>
<td></td>
<td>your mouse pointer over the value to view a list of associated NetBIOS</td>
</tr>
<tr>
<td></td>
<td>names.</td>
</tr>
<tr>
<td><strong>DNS Name</strong></td>
<td>Displays the IP address or DNS name of the asset, if known. If the asset</td>
</tr>
<tr>
<td></td>
<td>has more than one DNS name, this field indicates the number of DNS names.</td>
</tr>
<tr>
<td></td>
<td>Move your mouse pointer over the value to view a list of associated DNS</td>
</tr>
<tr>
<td></td>
<td>names.</td>
</tr>
<tr>
<td><strong>Given Name</strong></td>
<td>Displays the name of the asset. By default, this field is empty. To provide</td>
</tr>
<tr>
<td></td>
<td>a given name for the asset, edit the asset profile.</td>
</tr>
<tr>
<td><strong>Group Name</strong></td>
<td>Displays the last known user group of the asset, if known.</td>
</tr>
<tr>
<td><strong>Last User</strong></td>
<td>Displays the last known user of the asset. User information is derived from</td>
</tr>
<tr>
<td></td>
<td>identity events. If more than one user is associated with this asset, you</td>
</tr>
<tr>
<td></td>
<td>can click the link to display all users.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>Displays the operating system that is 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. You can edit this parameter directly if the Override parameter is specified as Until the Next Scan or Forever.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the level of importance that is 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.</td>
</tr>
</tbody>
</table>
| 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" on page 97.  
  For more information about 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.                                                                                                                                                     |
| 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. 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.                                                                                                       |
## Network Interface Summary pane

You can find Parameter descriptions for the Network Interface Summary pane that you access from the Asset Profile page.

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

### Table 1 Network Interface Summary pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address of this asset, if known.</td>
</tr>
</tbody>
</table>

Chapter 9. Accessing asset profile information  111
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Displays the IP address that is detected for this MAC address.</td>
</tr>
<tr>
<td>Network</td>
<td>Displays the network the IP address is associated with, if known.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Displays the date and time the IP address was last detected on this MAC address.</td>
</tr>
</tbody>
</table>

**Vulnerability pane**

You can find Parameter descriptions for the Vulnerability pane that you access from the Asset Profile page.

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

*Table 35. Vulnerability pane parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Displays the ID of the vulnerability. The ID is a unique identifier that is generated by Vulnerability Information System (VIS).</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the Payment Security Industry (PCI) severity that is associated to vulnerability.</td>
</tr>
<tr>
<td>Risk</td>
<td>Risk level that is associated to vulnerability. Sorting on this column must be by the underlying risk level code</td>
</tr>
<tr>
<td>Service</td>
<td>Service that is associated to the vulnerability (as discovered by scan). If only 1 service is associated, then display the service. Otherwise, display Multiple (N) where N indicates to total number of services associated to this vulnerability.</td>
</tr>
<tr>
<td>Port</td>
<td>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.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Name or title of this vulnerability.</td>
</tr>
<tr>
<td>Details</td>
<td>Specific detailed text that is associated to this vulnerability as determined by scan. If only 1 Detail is associated, then display the text of this Detail. Otherwise, display Multiple (N) where N indicates to total number of Details that are associated to this vulnerability.</td>
</tr>
</tbody>
</table>
Table 35. Vulnerability pane parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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” on page 97.  
For more information about CVSS, see [http://www.first.org/cvss/](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

You can find Parameter descriptions for the Services pane that you access from the Asset Profile page.

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

Table 36. Services pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Displays the name of the open service.</td>
</tr>
<tr>
<td>Product</td>
<td>Displays the product that runs on this service, if known.</td>
</tr>
<tr>
<td>Port</td>
<td>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.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Displays a comma-separated list of protocols that are discovered on the port that runs the open service.</td>
</tr>
<tr>
<td>Last Seen Passive</td>
<td>Displays the date and time that the open service was last passively seen.</td>
</tr>
</tbody>
</table>
Table 36. Services pane parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen Active</td>
<td>Displays the date and time that the open service was last actively seen.</td>
</tr>
<tr>
<td>Service Default Ports</td>
<td>Displays a comma-separated list of known ports the Layer 7 application is known to run on.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Displays the number of vulnerabilities that are associated with this open service.</td>
</tr>
</tbody>
</table>

**Windows Services pane**

You can find Parameter descriptions for the Windows Services pane that you access from the Asset Profile page. 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 37. Windows Services pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the Windows service that was actively seen on the asset.</td>
</tr>
</tbody>
</table>
| Status    | Displays the status of the Windows service. Options include:  
• Enabled  
• Manual  
• Disabled |

**Packages pane**

You can find Parameter descriptions for the Packages pane that you access from the Asset Profile page.

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 38. Packages pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packages</td>
<td>Displays the name of the package that is applied to the asset.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version of the package that is applied to the asset.</td>
</tr>
<tr>
<td>Revision</td>
<td>Displays the revision of the package that is applied to the asset.</td>
</tr>
</tbody>
</table>

**Windows Patches pane**

You can find Parameter descriptions for the Windows Patches pane that you access from the Asset Profile page.
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 39. Windows Patches pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft KB Number</td>
<td>Displays the Microsoft Knowledge Base (KB) number of the Windows patch that runs on the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the Windows patch.</td>
</tr>
<tr>
<td>Bulletin ID</td>
<td>Displays the bulletin ID number of the Windows patch.</td>
</tr>
<tr>
<td>Vulnerability ID</td>
<td>Displays the vulnerability ID of the Windows patch.</td>
</tr>
<tr>
<td>CVE-ID</td>
<td>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.</td>
</tr>
<tr>
<td>System</td>
<td>Displays the Windows system for the patch.</td>
</tr>
<tr>
<td>Service Pack</td>
<td>Displays the service pack for the patch.</td>
</tr>
</tbody>
</table>

Properties pane

You can find Parameter descriptions for the Properties pane that you access from the Asset Profile page. 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 40. Properties pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the configuration property that was actively seen on the asset.</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the value for the configuration property.</td>
</tr>
</tbody>
</table>

Risk Policies pane

You can find Parameter descriptions for the Risk Policies pane that you access from the Asset Profile page. 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 41. Risk Policies pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Displays the name of the policy that is associated with this asset.</td>
</tr>
</tbody>
</table>
Table 41. Risk Policies pane parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass/Fail</td>
<td>Indicates whether the policy has a status of Pass or Fail.</td>
</tr>
<tr>
<td>Last Evaluated</td>
<td>Displays the date that this policy was last evaluated.</td>
</tr>
</tbody>
</table>

Products pane

You can find Parameter descriptions for the Products pane that you access from the Asset Profile page.

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

Table 42. Products pane parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Displays the name of the product that runs on the asset.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port that the product uses.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Displays the number of vulnerabilities that are associated with this product.</td>
</tr>
<tr>
<td>Vulnerability ID</td>
<td>Displays the vulnerability ID.</td>
</tr>
</tbody>
</table>
Chapter 10. Report management

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

Detailed, flexible reporting options satisfy your various regulatory standards, such as PCI compliance.

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.

The Reports tab might require an extended period of time to refresh if your system includes many 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 session must be synchronized with your timezone.

During the installation and setup of QRadar products, the time zone is configured. Check with your administrator to ensure your QRadar session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report 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.

If a report does not specify an interval schedule, you must manually generate the report.

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.

Reports tab overview

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.
The Reports tab might require an extended period of time to refresh if your system includes many 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 session must be synchronized with your timezone.

During the installation and setup of QRadar products, the time zone is configured. Check with your administrator to ensure your QRadar session is synchronized with your timezone.

Report tab permissions
Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report 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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag Column</td>
<td>If an error occurred, causing the report generation to fail, the <strong>Error</strong> icon is displayed in this column.</td>
</tr>
<tr>
<td>Report Name</td>
<td>Specifies the report name.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the group to which this report belongs.</td>
</tr>
<tr>
<td>Schedule</td>
<td>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.</td>
</tr>
<tr>
<td>Next Run Time</td>
<td>Specifies the duration of time, in hours and minutes, until the next report is generated.</td>
</tr>
<tr>
<td>Last Modification</td>
<td>Specifies the last date that this report was modified.</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the user that owns the report.</td>
</tr>
<tr>
<td>Author</td>
<td>Specifies the user that created the report.</td>
</tr>
</tbody>
</table>
Table 43. Report tab parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated Reports</td>
<td>From this list box, select the date stamp of the generated report that you want to view. When you select the date stamp, the Format parameter displays the available formats for the generated reports. If no reports have been generated, None is displayed.</td>
</tr>
<tr>
<td>Formats</td>
<td>Specifies the report formats of the currently selected report in the Generated Reports column. Click the icon for the format you want to view.</td>
</tr>
</tbody>
</table>

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.

Report 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 44. Report toolbar options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Manage Groups</td>
<td>Click Manage Groups to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Actions</td>
<td>Click Actions to perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Create - Select this option to create a new report.</td>
</tr>
<tr>
<td></td>
<td>• Edit - Select this option to edit the selected report. You can also double-click a report to edit the content.</td>
</tr>
<tr>
<td></td>
<td>• Duplicate - Select this option to duplicate or rename the selected report.</td>
</tr>
<tr>
<td></td>
<td>• Assign Groups - Select this option to assign the selected report to a report group.</td>
</tr>
<tr>
<td></td>
<td>• Share - Select this option to share the selected report with other users. You must have administrative privileges to share reports.</td>
</tr>
<tr>
<td></td>
<td>• Toggle Scheduling - Select this option to toggle the selected report to the Active or Inactive state.</td>
</tr>
<tr>
<td></td>
<td>• Run Report - Select this option to generate the selected report. To generate multiple reports, hold the Control key and click on the reports you want to generate.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Hide Interactive Reports</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 44. Report toolbar options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Group  
- 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 various 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 many 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 Chart 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.

You can use any of the following types of charts:

- **None** - Use this option to display an empty container 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.

- **Asset Vulnerabilities** - Use this chart to view vulnerability data for each defined asset in your deployment. You can generate Asset Vulnerability charts when vulnerabilities have been detected by a VA scan. This chart is available after you install IBM Security QRadar Vulnerability Manager.

- **Vulnerabilities** - The Vulnerabilities option is only displayed when the IBM Security QRadar Vulnerability Manager has been purchased and licensed. For more information, see the IBM Security QRadar Vulnerability Manager User Guide.

For more information on these chart types, see Chart container parameters.
Graph types

Each chart type supports various graph types you can use to display data.

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

You can use the Report wizard to create a new report.

Before you begin

You must have appropriate network permissions to share a generated report with other users.

For more information about permissions, see the IBM Security QRadar Log Manager Administration Guide.

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 seven days to build the data. This search does not return results before seven days has elapsed.

When you specify the output format for the report, consider that the file size of generated reports can be one to 2 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

1. Click the Reports tab.
2. From the Actions list box, select Create.
3. On the Welcome to the Report wizard change, click Next to move to the next page of the Report wizard.
4. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually</td>
<td>Generates a report once. This is the default setting; however, you can generate this report as often as required.</td>
</tr>
<tr>
<td>Hourly</td>
<td>Schedules the report to generate at the end of each hour using the data from the previous hour.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Schedules the report to generate weekly using the data from the previous week.</td>
</tr>
<tr>
<td></td>
<td>If you choose the Weekly option, further configuration is required. Select the day that 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.</td>
</tr>
<tr>
<td>Monthly</td>
<td>Schedules the report to generate monthly using the data from the previous month.</td>
</tr>
<tr>
<td></td>
<td>If you choose the Monthly option, further configuration is required. From the list box, select the date that 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.</td>
</tr>
</tbody>
</table>

5. In the Allow this report to generate manually pane, Yes or No.
6. Configure the layout of your report:
   a. From the Orientation list box, select the page orientation: Portrait or Landscape.
   b. Select one of the six layout options that are displayed on the Report wizard.
   c. Click Next to move to the next page of the Report wizard.
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.
8. Configure each container in the report:
   a. From the Chart Type list box, select a chart type.
b. On the Container Details - <chart_type> window, configure the chart parameters.

c. Click **Save Container Details**.

d. If required, repeat steps a to c for all containers.

e. Click **Next** to move to the next page of the Report wizard.

9. Preview the Layout Preview page, and then click **Next** to move to the next step of the Report wizard.

10. Select the check boxes for the report formats you want to generate, and then click **Next**.

    **Note:** Extensible Markup Language is only available for tables.

11. Select the distribution channels for your report, and then click **Next**. Options include the following distribution channels:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Console</td>
<td>Select this check box to send the generated report to the <strong>Reports</strong> tab. This is the default distribution channel.</td>
</tr>
<tr>
<td>Select the users that should be able to view the generated report.</td>
<td>This option displays after you select the <strong>Report Console</strong> check box. From the list of users, select the users that you want to grant permission to view the generated reports.</td>
</tr>
<tr>
<td>Select all users</td>
<td>This option is only displayed after you select the <strong>Report Console</strong> check box. Select this check box if you want to grant permission to all users to view the generated reports. You must have appropriate network permissions to share the generated report with other users.</td>
</tr>
<tr>
<td>Email</td>
<td>Select this check box if you want to distribute the generated report using email.</td>
</tr>
<tr>
<td>Enter the report distribution email address(es)</td>
<td>This option is only displayed after you select the <strong>Email</strong> 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 are 255. Email recipients receive this email from no_reply_reports@qradar.</td>
</tr>
<tr>
<td>Include Report as attachment (non-HTML only)</td>
<td>This option is only displayed after you select the <strong>Email</strong> check box. Select this check box to send the generated report as an attachment.</td>
</tr>
<tr>
<td>Include link to Report Console</td>
<td>This option is only displayed after you select the <strong>Email</strong> check box. Select this check box to include a link the Report Console in the email.</td>
</tr>
</tbody>
</table>

12. On the Finishing Up page, enter values for the following parameters:
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Description</td>
<td>Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.</td>
</tr>
<tr>
<td>Groups</td>
<td>Select the groups to which you want to assign this report. For more information about groups, see <a href="#">Report groups</a>.</td>
</tr>
<tr>
<td>Would you like to run the report now?</td>
<td>Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.</td>
</tr>
</tbody>
</table>

13. Click **Next** to view the report summary.


### Results

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 reconfigure 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

You use the Reports tab and the Reports wizard to manage 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

You can use or customize a significant number of default reports. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.

#### Procedure

1. Click the **Reports** tab.
2. Double-click the report that you want to customize.
3. On the Report wizard, change the parameters to customize the report to generate the content you require.

### Results

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, which is 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 PDF, HTML, RTF, XML, and XLS formats.

Note: 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 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 starts a new browser window. This new window launch is the result of the Mozilla Firefox web browser configuration and does not affect QRadar. You can close the window and continue with your QRadar session.

Procedure

1. Click the Reports tab.
2. From the list box in the Generated Reports column, select the time-stamp of report you want to view.
3. Click the icon for the format you want to view.

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

1. Click the Reports tab.
2. Select the reports for which you want to delete the generated content.
3. From the Actions list box, click Delete Generated Content.

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 that 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
1. Click the Reports tab.
2. Select the report that you want to generate.
3. Click Run Report.

What to do next
After the report generates, you can view the generated report from the Generated Reports column.

Duplicating a report
To create a report that closely resembles an existing report, you can duplicate the report that you want to model, and then customize it.

Procedure
1. Click the Reports tab.
2. Select the report that you want to duplicate.
3. From the Actions list box, click Duplicate.
4. Type a new name, without spaces, for the report.

What to do next
You can customize the duplicated 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.

You can only share the report with users that have the appropriate access.

Procedure
1. Click the Reports tab.
2. Select the reports that you want to share.
3. From the Actions list box, click Share.
4. From the list of users, select the users with whom you want to share this report.

**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 that 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, 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**

1. Click the **Reports** tab.
2. On the navigation menu, click **Branding**.
3. Click **Browse** to browse the files that are located on your system.
4. Select the file that contains the logo you want to upload. Click **Open**.
5. Click **Upload Image**.
6. Select the logo that you want to use as the default and click **Set Default Image**.

**Report groups**

You can sort reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports.

For example, you can view all reports that are 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
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 report group

You can create new groups.

Procedure
1. Click the Reports tab.
2. Click Manage Groups.
3. Using the navigation tree, select the group under which you want to create a new group.
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 - Optional. Type a description for this group. The description can be up to 255 characters in length.
6. Click OK.
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.

Editing a group

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

Procedure
1. Click the Reports tab.
2. Click Manage Groups.
3. From the navigation tree, select the group that you want to edit.
4. Click Edit.
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 - Optional. Type a description for this group. The description can be up to 255 characters in length. This field is optional.
6. Click OK.

Assign a report to a group

You can use the Assign Groups option to assign a report to another group.
**Procedure**

1. Click the **Reports** tab.
2. Select the report that you want to assign to a group.
3. From the **Actions** list box, select **Assign Groups**.
4. From the **Item Groups** list, select the check box of the group you want to assign to this report.
5. Click **Assign Groups**.

**Copying a report to another group**

Use the **Copy** icon to copy a report to one or more report groups.

**Procedure**

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, select the report that you want to copy.
4. Click **Copy**.
5. Select the group or groups to which you want to copy the report.
6. Click **Assign Groups**.

**Removing a report**

Use the **Remove** icon to 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**

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, navigate to the folder that contains the report you want to remove.
4. From the list of groups, select the report that you want to remove.
5. Click **Remove**.
6. Click **OK**.

**Chart container**

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.
Asset Vulnerabilities chart container parameters

The following table describes the Asset Vulnerabilities chart container parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Container Details - Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Chart Title</td>
<td>Type a chart title to a maximum of 100 characters.</td>
</tr>
<tr>
<td>Chart Sub-Title</td>
<td>Clear the check box to change the automatically created subtitle. Type a title to a maximum of 100 characters.</td>
</tr>
<tr>
<td>Limit Assets to Top</td>
<td>From the list box, select how many assets you want to include in this report.</td>
</tr>
<tr>
<td><strong>Graph Type</strong></td>
<td>From the list box, select the type of graph to display on the generated report. Options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Aggregate Table</strong> - Displays the data in an aggregated table, which is a table that contains subtables (subreports). When you select this option, you must configure the subreport details. The <strong>Table</strong> option is only available for the full page width container.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Bar</strong> - Displays the data in a bar chart. When you select this option, the report does not include subreport data. This is the default. This graph type requires the saved search to be a grouped search.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Pie</strong> - Displays the data in a pie chart. When you select this option, the report does not include subreport data. This graph type requires the saved search to be a grouped search.</td>
</tr>
<tr>
<td><strong>Order Assets By</strong></td>
<td>Select the type of data on which you want the chart to be ordered. Options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Asset Weight</strong> - Orders the data by the asset weight that is defined in the asset profile.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CVSS Risk</strong> - Orders the data by the Common Vulnerability Scoring System (CVSS) risk level. For more information about CVSS, see <a href="http://www.first.org/cvss">http://www.first.org/cvss</a>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Vulnerability Count</strong> - Orders the data by the vulnerability count of the assets.</td>
</tr>
<tr>
<td><strong>Sub-Report Details</strong></td>
<td>Specifies the type of information that displays in the subreport.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order Subreport By</td>
<td>Select the parameter by which you want to organize the subreport data. The options include:</td>
</tr>
<tr>
<td></td>
<td>• Risk (Base Score)</td>
</tr>
<tr>
<td></td>
<td>• OSVDB ID</td>
</tr>
<tr>
<td></td>
<td>• OSVDB Title</td>
</tr>
<tr>
<td></td>
<td>• Last Modified Date</td>
</tr>
<tr>
<td></td>
<td>• Disclosure Date</td>
</tr>
<tr>
<td></td>
<td>• Discovery Date</td>
</tr>
<tr>
<td></td>
<td>For more information about the Open Source Vulnerability Database (OSVDB), see <a href="http://osvdb.org/">http://osvdb.org/</a>.</td>
</tr>
<tr>
<td>Limit Sub-report to Top</td>
<td>From the list box, select how many vulnerabilities you want to include in this sub-report.</td>
</tr>
<tr>
<td>Graph Content</td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>To specify the vulnerabilities, you want to report:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Browse</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. From the <strong>Search by</strong> list box, select the vulnerability attribute that you want to search by. Options include CVE ID, Bugtraq ID, OSVDB ID, and OSVDB Title. For more information about vulnerability attributes, see <a href="https://assetmanagement">Asset Management</a>.</td>
</tr>
<tr>
<td></td>
<td>3. From the <strong>Search Results</strong> list, select the vulnerabilities that you want to report. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Submit</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Type the IP address, CIDR, or a comma-delimited list of IP addresses you want to report. Partial CIDRs are permitted.</td>
</tr>
<tr>
<td>Networks</td>
<td>From the navigation tree, select one or more networks from which to gather chart data.</td>
</tr>
</tbody>
</table>

### Event/Logs chart container parameters

The following table describes the Events/Logs chart container parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Container Details - Events/Logs</strong></td>
<td></td>
</tr>
<tr>
<td>Chart Title</td>
<td>Type a chart title to a maximum of 100 characters.</td>
</tr>
<tr>
<td>Chart Sub-Title</td>
<td>Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Limit Events/Logs to Top</td>
<td>From the list box, select the number of events/logs to be displayed in the generated report.</td>
</tr>
<tr>
<td>Graph Type</td>
<td>From the list box, select the type of graph to display on the generated report. Options include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bar</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Line</strong> - Displays the data in a line chart.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pie</strong> - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stacked Bar</strong> - Displays the data in a stacked bar chart.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stacked Line</strong> - Displays the data in a stacked line chart.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table</strong> - Displays the data in table format. The <strong>Table</strong> option is only available for the full page width container only.</td>
</tr>
</tbody>
</table>

To view examples of each graph charts data type, see [See Graph types](#).
Table 45. Event/Logs chart container parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Scheduling</td>
<td>The Manual Scheduling pane is displayed only if you selected the <strong>Manually</strong> scheduling option in the Report wizard.</td>
</tr>
<tr>
<td></td>
<td>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 that is generated during your business hours, such as Monday to Friday, 8 AM to 9 PM.</td>
</tr>
<tr>
<td></td>
<td>To create a manual schedule:</td>
</tr>
<tr>
<td>1.</td>
<td>From the <strong>From</strong> list box, type the start date that you want for the report, or select the date using the Calendar icon. The default is the current date.</td>
</tr>
<tr>
<td>2.</td>
<td>From the list boxes, select the start time that you want for the report. Time is available in half-hour increments. The default is 1:00 a.m.</td>
</tr>
<tr>
<td>3.</td>
<td>From the <strong>To</strong> list box, type the end date you want for the report, or select the date using the Calendar icon. The default is the current date.</td>
</tr>
<tr>
<td>4.</td>
<td>From the list boxes, select the end time that you want for the report. Time is available in half-hour increments. The default is 1:00 a.m.</td>
</tr>
<tr>
<td>5.</td>
<td>From the <strong>Timezone</strong> list box, select the time zone that you want to use for your report.</td>
</tr>
<tr>
<td>6.</td>
<td>When configuring the <strong>Timezone</strong> parameter, consider the location of the Event Processors that are 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 <strong>GMT -5.00 America/New_York</strong>, the data from Europe reports the time zone incorrectly.</td>
</tr>
</tbody>
</table>
Table 45. Event/Logs chart container parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manual Scheduling (continued) | 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 that 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. |
| 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 that you want to use for your report.  
• 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. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Scheduling</td>
<td>The Daily Scheduling pane is displayed only if you selected the <strong>Daily</strong> scheduling option in the Report wizard.</td>
</tr>
<tr>
<td></td>
<td>1. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>2. <strong>All data from previous day (24 hours)</strong></td>
</tr>
<tr>
<td></td>
<td>3. <strong>Data of previous day from</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Timezone</strong> list box, select the time zone that you want to use for your report.</td>
</tr>
<tr>
<td></td>
<td>5. When configuring the <strong>Timezone</strong> 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 <strong>GMT -5.00 America/New_York</strong>, the data from Europe reports the time zone incorrectly.</td>
</tr>
</tbody>
</table>
Table 45. Event/Logs chart container parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Scheduling</td>
<td>The Weekly Scheduling pane is displayed only if you selected the Weekly scheduling option in the Report wizard.</td>
</tr>
<tr>
<td></td>
<td>1. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>2. All data from previous week</td>
</tr>
<tr>
<td></td>
<td>3. 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.</td>
</tr>
<tr>
<td></td>
<td>4. From the Timezone list box, select the time zone that you want to use for your report.</td>
</tr>
<tr>
<td></td>
<td>5. 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To further refine your schedule:</td>
</tr>
<tr>
<td></td>
<td>1. Select the Targeted Data Selection check box. More options are displayed.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Only hours from check box, and then using the list boxes, select the time range that you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM.</td>
</tr>
<tr>
<td></td>
<td>3. Select the check box for each day of the week you want to schedule your report for.</td>
</tr>
</tbody>
</table>
### Table 45. Event/Logs chart container parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monthly Scheduling</strong></td>
<td>The Monthly Scheduling pane is displayed only if you selected the <em>Monthly</em> scheduling option in the Report wizard.</td>
</tr>
<tr>
<td></td>
<td>1. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>2. <strong>All data from previous month</strong></td>
</tr>
<tr>
<td></td>
<td>3. <strong>Data from previous month from the</strong> - From the list boxes, select the period of time you want for the generated report. The default is 1st to 31st.</td>
</tr>
<tr>
<td></td>
<td>4. From the <strong>Timezone</strong> list box, select the time zone that you want to use for your report.</td>
</tr>
<tr>
<td></td>
<td>5. When configuring the <strong>Timezone</strong> 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 <strong>GMT -5.00 America/New_York</strong>, the data from Europe reports the time zone incorrectly.</td>
</tr>
<tr>
<td></td>
<td>To further refine your schedule:</td>
</tr>
<tr>
<td></td>
<td>1. Select the <strong>Targeted Data Selection</strong> check box. More options are displayed.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Only hours from</strong> check box, and then using the list boxes, select the time range that you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM.</td>
</tr>
<tr>
<td></td>
<td>3. Select the check box for each day of the week you want to schedule your report for.</td>
</tr>
</tbody>
</table>

#### 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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Saved Searches</td>
<td>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.</td>
</tr>
<tr>
<td>Create New Event Search</td>
<td>Click Create New Event Search to create a new search. For more information about how to create an event search, see Log activity investigation.</td>
</tr>
</tbody>
</table>
Notices

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

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

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

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to 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 may not appear.

**Trademarks**

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols
Privacy policy considerations

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

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

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

Glossary

This glossary provides terms and definitions for the IBM Security QRadar SIEM software and products.

The following cross-references are used in this glossary:

- **See** refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- **See also** refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

**A**

**accumulator**
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

**active system**
In a high-availability (HA) cluster, the system that has all of its services running.

**Address Resolution Protocol (ARP)**
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

**anomaly**
A deviation from the expected behavior of the network.

**application signature**
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

**ARP**
See Address Resolution Protocol

**ARP Redirect**
An ARP method for notifying the host if a problem exists on a network.

**ASN**
See autonomous system number

**autonomous system number (ASN)**
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

**B**

**behavior**
The observable effects of an operation or event, including its results.

**C**

**CIDR**
See Classless Inter-Domain Routing

**Classless Inter-Domain Routing (CIDR)**
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

**client**
A software program or computer that requests services from a server.

**cluster virtual IP address**
An IP address that is shared between the primary or secondary host and the HA cluster.

**coalescing interval**
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.
Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

F

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.
### G

**gateway**
A device or program used to connect networks or systems with different network architectures.

### H

**HA**  
See [high availability](#).

**HA cluster**
A high-availability configuration consisting of a primary server and one secondary server.

**Hash-Based Message Authentication Code (HMAC)**
A cryptographic code that uses a cryptic hash function and a secret key.

**high availability (HA)**
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

**HMAC**  
See [Hash-Based Message Authentication Code](#).

**host context**
A service that monitors components to ensure that each component is operating as expected.

### I

**ICMP**  
See [Internet Control Message Protocol](#).

**identity**
A collection of attributes from a data source that represent a person, organization, place, or item.

**IDS**  
See [intrusion detection system](#).

**Internet Control Message Protocol (ICMP)**
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

**Internet Protocol (IP)**
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

**Internet service provider (ISP)**
An organization that provides access to the Internet.

**intrusion detection system (IDS)**
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

**intrusion prevention system (IPS)**
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

**IP**  
See [Internet Protocol](#).

**IP multicast**
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

**IPS**  
See [intrusion prevention system](#).

**ISP**  
See [Internet service provider](#).

### L

**L2L**  
See [Local To Local](#).

**L2R**  
See [Local To Remote](#).

**LAN**  
See [local area network](#).

**LDAP**  
See [Lightweight Directory Access Protocol](#).

**leaf**
In a tree, an entry or node that has no children.

**Lightweight Directory Access Protocol (LDAP)**
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

**local area network (LAN)**
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.
Local To Local (L2L)
  Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
  Pertaining to the internal traffic from one local network to another remote network.

log source
  Either the security equipment or the network equipment from which an event log originates.

magistrate
  An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
  A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

NetFlow
  A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

Network Address Translation (NAT)
  In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
  A type of container that is a hierarchical collection of network objects.

network layer
  In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
  A component of a network hierarchy.

network weight
  The numeric value applied to each network that signifies the importance of the network. The network weight is defined by the user.

offense
  A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
  A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
  A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
  Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
  The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
  See open systems interconnection.

OSVDB
  See Open Source Vulnerability Database.

payload data
  Application data contained in an IP flow, excluding header and administrative information.

primary HA host
  The main computer that is connected to the HA cluster.

protocol
  A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.
Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L  See Remote To Local
R2R  See Remote To Remote

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report
In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork

subnet mask
For internet subnetworking, a 32-bit mask
used to identify the subnetwork address
bits in the host portion of an IP address.

**subnetwork (subnet)**
A network that is divided into smaller
independent subgroups, which still are
interconnected.

**sub-search**
A function that allows a search query to
be performed within a set of completed
search results.

**superflow**
A single flow that is comprised of
multiple flows with similar properties in
order to increase processing capacity by
reducing storage constraints.

**system view**
A visual representation of both primary
and managed hosts that compose a
system.

---

**T**

**TCP**  See [Transmission Control Protocol](#)

**Transmission Control Protocol (TCP)**
A communication protocol used in the
Internet and in any network that follows
the Internet Engineering Task Force (IETF)
standards for internetwork protocol. TCP
provides a reliable host-to-host protocol in
packet-switched communication networks
and in interconnected systems of such
networks. See also [Internet Protocol](#)

---

**V**

**violation**
An act that bypasses or contravenes
corporate policy.

---

**W**

**whois server**
A server that is used to retrieve
information about a registered Internet
resources, such as domain names and IP
address allocations.
Index

A
add asset 91, 97
add filter 58
add items 16, 20
adding event items 20
adding flow search items 20
Admin tab 5
Aggregate CVSS score 92
anomaly detection rule 76
Anomaly Detection Rule wizard 76
asset 93
Asset name 92
asset profile 95, 97
Asset Profile page 106, 109, 111, 113, 114, 115, 116
Asset profile page parameters 109
asset profiles 91, 102, 103, 105, 106
Asset profiles 93, 104
Asset Profiles 103, 104
Asset profiles page 92
asset search groups 103
asset search page 101
Asset Summary pane parameters 109
Asset tab 91, 92, 95, 103
asset vulnerabilities 106
assets 5, 12, 13
assets tab 97, 103, 105
Assets tab 5, 91, 93, 95, 103, 104, 105
assign items to a group 81

B
browser mode
   Internet Explorer web browser 3
building blocks 73
editing 82

calculated property type 65
calculation property 68
cancel a search 61
Chart container 130
chart legends 49
chart objects 49
chart types 121
charts overview 47
configure and manage networks, plug-ins and components 5
configure and manage systems 5
configure and manage users 5
configure page size 13
configuring charts 49
configuring connections 17
configuring dashboard items 17
configuring log activity 17
console time 11
do not hallucinate.
controls 6
copy a rule 79
copy an item to a group 81
copy saved search 63, 104
create a rule group 80
create new search group 103
create reports 5
creating a new search group 63
creating custom rules 75
creating search groups 62
custom event properties 65
custom property 71
custom reports 122
custom rules wizard 6
Custom Rules Wizard 15
distribute reports 5
document mode
   Internet Explorer web browser 3
download PCAP data file 44
download PCAP file 45
Duplicate a report 127
eexporting assets 106
exporting events 45

F
false positives 91
Flag 15
flows 49, 51
functions 73

generate a report manually 126
glossary 145
graph types 122
group
assigning items 81
editing 81
deleting 82
deleting an item 82
document mode
   Internet Explorer web browser 3
download PCAP data file 44
download PCAP file 45
duplicate a report 127
e export a report 127
eimport asset profile 105
eimport assets 105
introduction vii
ip address 9, 92
image
   reports
      branding 128
      upload 128
import asset profile 105
import assets 105
investigate asset 91
investigate event logs 4
investigate log activity 23
investigating events 13
IP address 9, 92

L
last minute (auto refresh) 8
list of events 38
log activity 8, 12, 13, 17, 20, 23, 42, 47,
   49, 51, 58, 59, 61, 62, 63, 65, 73
   overview 23
search criteria 56
Log Activity dashboard items 13
M
maintain custom rule 73
maintain custom rules 73
Manage Groups 104
manage network 91
manage reports 5, 119
manage search results 61, 62
managing search groups 62
map event 42
messages menu 6
modify event mapping 42
monitoring events 13
Most recent reports generated 15
multiple dashboards 13

N
navigate QRadar 3
network activity 12, 20, 47, 49, 51, 58
network activity tab 8, 51
network administrator vii
Network Interface pane 109
Network Interface Summary pane parameters 111
new features
    version 7.2.2 user guide overview 1
new search 104
normalized events 29
notification message 15

O
offenses 13, 51, 63
offenses tab 8
online help 12
organize your dashboard items 13

P
Packages pane 109
Packages pane parameters 114
Packet Capture (PCAP) data 43
password 4
pause data 8
PCAP data 43, 44
PCAP data column 43, 45
performing a sub-search 58
permissions 118
custom properties 65
play data 8
print asset profile 91
Products pane 109
Products pane parameters 116
properties pane 109
Properties pane parameters 115
property
    copying custom 71
property (continued)
    modifying custom 69
property types 65

Q
QID 42
QRadar Vulnerability Manager 91
quick filter 27, 51

R
raw event data 32
real time (streaming) 8
real-time 28
refresh data 8
regex property 66
regex property type 65
remove group 64, 104
Remove icon 104
remove item from dashboard 18
remove saved search 104
remove saved search from a group 64
rename dashboard 19
report
    editing 125
    Report layout 121
    report tab 118, 119
    report tab parameters 118
    reports 12, 13
    viewing 126
    reports tab 8, 118
    Reports tab 5
    resize columns 12
    Rick Policies pane parameters 115
    right-click menu 27
    right-click menu options 95
    Risk Policies pane rule
        copying 79
        edit 79
        responses 74
        rule group
            creating 80
            viewing 80
            rule group management 80
            rule management 73, 78
            rule parameters 83
            rule permission 73
        Rule Response 85
        rules 73
        disabling 78
        enabling 78
        viewing 75
    rules page toolbar 84
search criteria (continued)
    deleting 57
    log activity tab 57
    saving 56
    search for asset 91
    search group
        creating 63
        editing 63
    search groups
        managing 62
        viewing 62
    search groups window 62
    search results
        cancel 61
        deleting 62
        saving 59
        viewing managed 59
    searching 51
    searching asset profiles 101
    servers 5
    Services 92
    Services pane 109
    Services pane parameters 113
    share reports 127
    show dashboard 18, 19
    single event details 38
    sort order 119
    sort results in tables 8
    specify chart type 17
    specify number of data objects to view 17
    status bar 28, 121
    streaming events 28
    summary of activity within past 24 hours 15
    synchronize time 118
    system notification 20
    System Notification dashboard item 15
    system notifications 6
    System Summary dashboard item 15
    system time 11

T
tables 13
tabs 4
tests 73
third-party scanners 91
time series chart 47
timezone 118
toolbar 23

U
unparsed event data 32
update user details 11
updated offenses 15
user information 11
user interface 4
user interface tabs 4, 6
user name 4
user names 10
V
view asset profile 95
view assets 91
view custom rules 73
view grouped events 33
view messages 6
view PCAP data 44
view rule group 80
view system notifications 20
viewing managed search results 59
viewing search groups 62, 103
viewing streaming events 28
vulnerabilities 91
Vulnerabilities 92
vulnerability details 106
Vulnerability Management dashboard 15
Vulnerability pane 109
Vulnerability pane parameters 112
W
web browser
   supported versions 3
what's new
   version 7.2.2 user guide overview 1
Window Service pane parameters 114
Windows Patches pane parameters 115
Windows Patches pane, 109