IBM QRadar

Basic Notes

Deepak Rawat
March /2024

IBM QRadar

IBM QRadar is a Security Information and Event Management (SIEM) solution that helps organizations in detecting and responding to security threats and incidents across their IT infrastructure. It provides centralized log management, real-time threat detection, and correlation capabilities to enhance security operations. Here's a detailed, point-wise introduction to IBM QRadar:

1. Overview: IBM QRadar is a comprehensive security intelligence platform designed to help security teams identify, investigate, and respond to security threats more effectively. It combines Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), and Security Orchestration Automation and Response (SOAR) functionalities.

2. SIEM Capabilities: QRadar's SIEM capabilities collect and analyze log data from various sources, including network devices, servers, applications, and endpoints. It helps in identifying potential security threats, policy violations, and compliance issues by correlating events and analyzing patterns.

3. User and Entity Behavior Analytics (UEBA): QRadar's UEBA module monitors user behavior and identifies anomalies or deviations from normal patterns. It helps in detecting insider threats, account compromises, and other advanced attacks by learning normal behavior and flagging unusual activities.

4. Security Orchestration Automation and Response (SOAR): QRadar's SOAR capabilities help automate and streamline security operations. It allows security teams to define playbooks for incident response, integrate with other security tools, and orchestrate actions to improve response efficiency.

5. Threat Intelligence: QRadar integrates with various threat intelligence sources, such as IBM X-Force, to enrich event data with global threat intelligence. This helps in identifying known threats and provides context to better understand potential security incidents.

6. Advanced Analytics and Machine Learning: QRadar leverages advanced analytics and machine learning algorithms to identify hidden patterns and correlations within large volumes of log data. This helps in detecting previously unknown threats and improving overall threat detection accuracy.

7. Compliance and Regulatory Support: QRadar assists organizations in meeting regulatory requirements by providing pre-built compliance reports and customizable dashboards. It helps in monitoring and maintaining compliance across various industries and jurisdictions.

8. Scalability and Flexibility: QRadar offers both on-premises and cloud deployment options, allowing organizations to choose the best fit for their needs. It can scale to handle large volumes of data and supports various data sources, making it suitable for organizations of all sizes.

9. Integration Capabilities: QRadar integrates with a wide range of security tools, including firewalls, intrusion prevention systems, endpoint security solutions, and more. This allows for a unified security approach and improves overall security posture.

10. Centralized Management and Reporting: QRadar provides a single console for managing and monitoring security across the entire IT infrastructure. It offers customizable dashboards and reports, enabling security teams to gain valuable insights and make data-driven decisions.

In summary, IBM QRadar is a powerful SIEM solution that helps organizations detect and respond to security threats more effectively. Its comprehensive features, including SIEM, UEBA, and SOAR capabilities, make it an essential tool for modern security operations centers.

- ## Installation:

Installing a QRadar appliance

Last Updated: 2023-05-27

Install a IBM® QRadar® Console or a managed host on a QRadar appliance or on your own appliance.

Software versions for all QRadar appliances in a deployment must be same version and fix level. Deployments that use different versions of software are not supported.

Before you begin

Ensure that the following requirements are met:

The required hardware is installed.

You have the required license key for your appliance.

A keyboard and monitor are connected by using the VGA connection.

If you want to configure bonded network interfaces, see Configuring bonded management interfaces.

If you are installing QRadar on a Unified Extensible Firmware Interface (UEFI) system, secure boot must be disabled.

Procedure

1. Type root at the login prompt to launch the installation wizard. Type password if you are prompted for a password.
2. Accept the End User License Agreement.
3. Select the appliance type:
   - Appliance Install
   - High Availability Appliance
4. If you selected High Availability Appliance complete the following steps:
   a. Select HA appliance (All models) 500 as the functionality.
   b. Select whether the high-availability (HA) appliance is a standby for a console or non-console appliance.
   c. Select Next.
5. If you did not choose High Availability Appliance, select the appliance assignment, and then select Next.
6. For the type of setup, select Normal Setup (default) or HA Recovery Setup, and set up the time.
7. If you selected HA Recovery Setup, enter the cluster virtual IP address.
8. Select the Internet Protocol version:
   - ipv4
   - ipv6

   If you selected ipv6, select manual or auto for the Configuration type.

   manual

   You must use a static IP address with a CIDR range.

   auto

   A static IP address with a CIDR range is generated with the Neighbor Discovery Protocol.

9. Select the bonded interface setup, if required.
10. Select the management interface.
11. In the wizard, enter a fully qualified domain name in the Hostname field.
    - **Important:**
      1) The hostname must not contain only numbers.
      2) The console and managed host (MH) cannot have the same hostname.
12. In the IP address field, enter a static IP address, or use the assigned IP address.

13. If you do not have an email server, enter localhost in the Email server name field.

14. Enter a root password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
15. If you are installing a Console, enter an admin password that meets the following criteria:
    - Contains at least 8 characters
    - Contains at least one uppercase character
    - Contains at least one lowercase character
    - Contains at least one digit
    - Contains at least one special character: @, #, ^, or *
16. Click Finish.
17. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.

18. If you are installing a Console, apply your license key.

a) Log in to QRadar as the admin user:
b) https://<IP_Address_QRadar>
c) Click Login.
d) On the navigation menu (☰), click Admin.
e) In the navigation pane, click System Configuration.
f) Click the System and License Management icon.
g) From the Display list box, select Licenses, and upload your license key.
h) Select the unallocated license and click Allocate System to License.
i) From the list of systems, select a system, and click Allocate System to License.

19. If you want to add managed hosts, see the IBM QRadar Administration Guide.

QRadar installations

Last Updated: 2023-01-23

There are two ways to install QRadar® on your hardware: a software installation, or an appliance installation.

Appliance installation

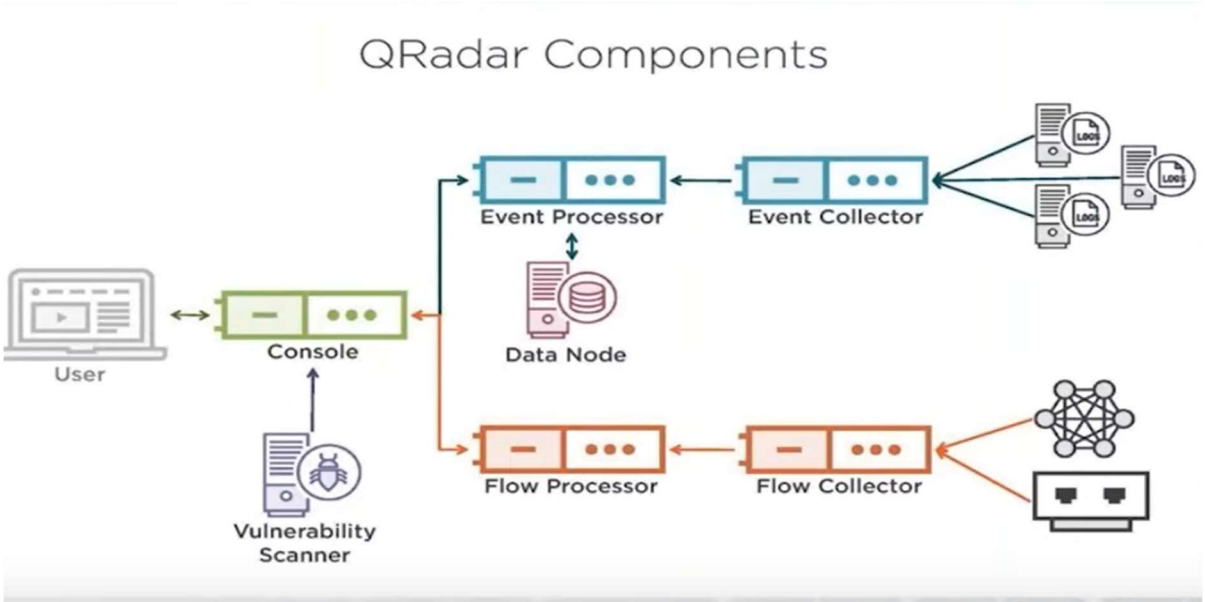
An appliance installation is a QRadar installation that uses the version of Red Hat® Enterprise Linux® (RHEL) included in the QRadar ISO. An appliance installation on your own hardware or in a virtual machine requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. You do not need to configure partitions or perform other RHEL preparation as part of an appliance installation. Choose this option, if RHEL is not already installed. Proceed to Installing a QRadar appliance. However, if the hardware/virtual instance configuration varies from our listed specifications, the version of RHEL included in the QRadar ISO may not install properly. In that case, you should attempt a software installation.

Software installation

A software installation is a QRadar installation that uses a RHEL operating system that you provide. The RHEL version required for your installment must be provided by a 3rd party. You must configure partitions and perform other RHEL preparations before a QRadar software installation. Aside from RHEL, all software installations requires you to purchase a software node entitlement. Contact your QRadar sales representative for more information about purchasing a software node entitlement. Proceed to QRadar software installations.

- **Installing a QRadar appliance**
  Install a IBM QRadar Console or a managed host on a QRadar appliance or on your own appliance.
- **QRadar software installations**
  A software installation is a QRadar installation on your hardware that uses an RHEL operating system that you provide. You must configure partitions and perform other RHEL preparation before a QRadar software installation.

Key Components of IBM QRadar:



Capabilities in your IBM QRadar product

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

IBM QRadar Log Manager

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

IBM QRadar SIEM

QRadar SIEM is an advanced offering that includes the full range of security intelligence capabilities for on-premises deployments. It consolidates log source and network flow data from thousands of assets, devices, endpoints, and applications that are distributed throughout your network, and performs

immediate normalization and correlation activities on the raw data to distinguish real threats from false positives.

IBM QRadar on Cloud

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

QRadar product capabilities

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

Table 1. Comparison of QRadar capabilities

Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Full administrative capabilities	Yes	No	Yes
Supports hosted deployments	No	Yes	No
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand-alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
Network activity monitoring	Yes	Yes	No
Asset profiling	Yes	Yes	No [1]
Offenses management	Yes	Yes	No

© Copyright IBM Corp. 2012, 2021

Table 1. Comparison of QRadar capabilities (continued)

Capability	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Network flow capture and analysis	Yes	Yes	No

Historical correlation	Yes	Yes	No
QRadar Network Insights integration	Yes	Yes	No
QRadar Vulnerability Manager integration	Yes	Yes	Yes
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No
Vulnerability assessment scanners	Yes	Yes	Yes
[1] QRadar Log Manager tracks asset data only if QRadar Vulnerability Manager is installed.			

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

Supported web browsers

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

The following table lists the supported versions of web browsers.

Table 2. Supported web browsers for QRadar products

Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported on QRadar 7.4.0 or later.

Security exceptions and certificates

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

Navigate the web-based application

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

IBM QRadar login

IBM 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 QRadar console.

Table 3. Default login information for QRadar

Login information	Default
URL	https://<IP Address>, where <IP Address> 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://[<IP Address>]
User name	admin
Password	The password that is assigned to QRadar during the installation process.
License key	A default license key provides you access to the system for 5 weeks.

RESTful API

The representational state transfer (REST) application programming interface (API) is useful when you want to integrate IBM QRadar with other solutions. You can perform actions on the QRadar Console by sending HTTPS requests to specific endpoints (URLs) on the QRadar Console.

Each endpoint contains the URL of the resource that you want to access and the action that you want to complete on that resource. The action is indicated by the HTTP method of the request: GET, POST, PUT, or DELETE. For more information about the parameters and responses for each endpoint, see the QRadar API Guide.

QRadar API forum and code samples

The API forum provides more information about the REST API, including the answers to frequently asked questions and annotated code samples that you can use in a test environment. For more information, see the API forum (https://ibm.biz/qradarforums).

QRadar common procedures

Various controls in QRadar are common to most tabs.

Viewing notifications

The **Notifications** menu 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 **Notifications** 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 over a notification to view more details. You can use the functions on the **Messages** window to manage the system notifications.

System notifications are also available on the **Dashboard** tab and on an optional pop-up window. 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.

Procedure

1. Log in to QRadar.
2. Click **Notifications**.
3. On the **Messages** window, view the system notification details.
4. To refine the list of system notifications, click one of the following options:
   - **Errors**
   - **Warnings**
   - **Info**
5. To close system notifications, choose one of the following options:

Option	Description
Dismiss All Info	Click to close all system notifications.
Dismiss	Click the **Dismiss** icon next to the system notification that you want to close.

6. To view the system notification details, hover over the system notification.

Related tasks

"Creating a custom rule" on page 185

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.

Refreshing and pausing QRadar

You can manually refresh, pause, and play the data that is displayed on tabs.

Dashboard tab

The **Dashboard** tab automatically refreshes every 60 seconds. The timer indicates the amount of time that remains until the tab is automatically refreshed. See Figure 7 for an example.

Click the title bar of any dashboard item to automatically pause the refresh time. The timer flashes red to indicate that the current display is paused.

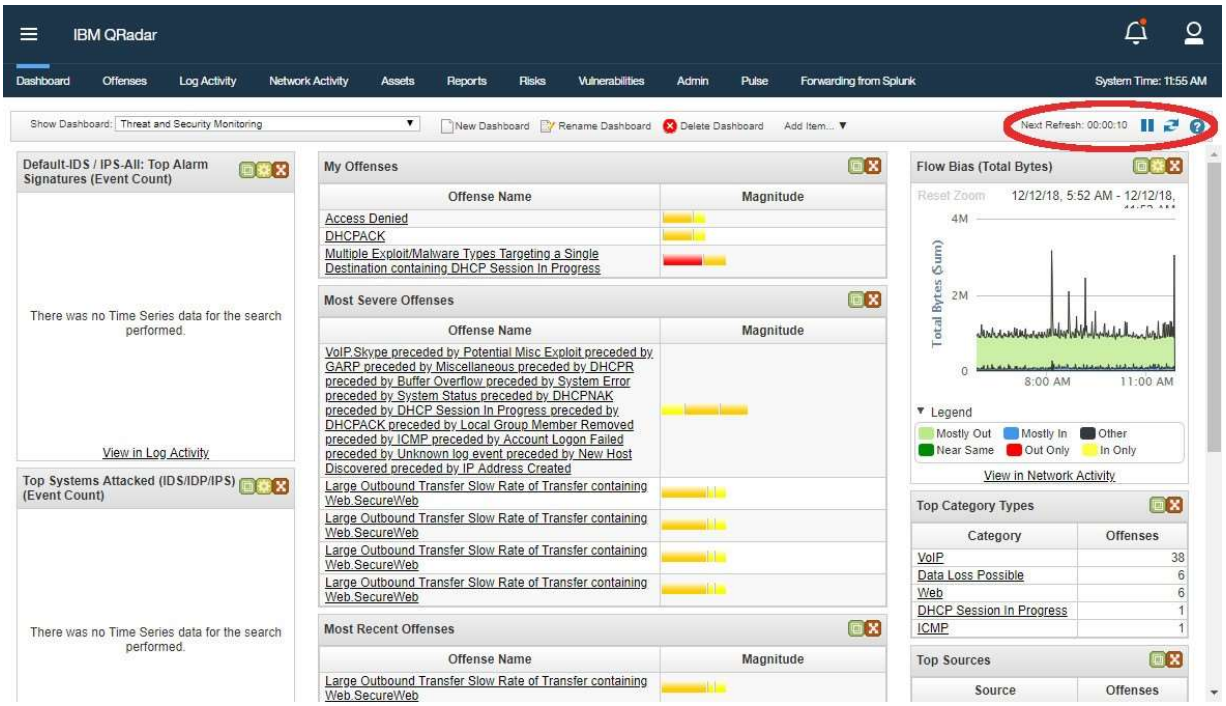


Figure 2. Timer in QRadar Console

Log Activity and Network Activity tabs

The **Log Activity** and **Network Activity** tabs automatically refresh every 60 seconds if you are viewing the tab in Last Interval (auto refresh) mode.

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

Offenses tab

The **Offenses** tab must be refreshed manually. The timer indicates the amount of time since the data was last refreshed. The timer flashes red when the timer is paused.

Investigating IP addresses

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

Procedure

1. Log in to QRadar.
2. Click the tab that you want to view.
3. Hover 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:

Table 4. IP addresses information

Option	Description
Navigate > **View by Network**	Displays the networks that are associated with the selected IP address.

Navigate > **View Source Summary**	Displays the offenses that are associated with the selected source IP address.
Navigate > **View Destination Summary**	Displays the offenses that are associated with the selected destination IP address.
Information > **DNS Lookup**	Searches for DNS entries that are based on the IP address.
Information > **WHOIS Lookup**	Searches for the registered owner of a remote IP address. The default whois server is whois.arin.net.
Information > **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.

Table 4. IP addresses information (continued)

Option	Description
Information > **Asset Profile**	Displays asset profile information. This option is displayed if IBM QRadar Vulnerability Manager is purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*. This menu option is available if QRadar acquired profile data either actively through a scan or passively through flow sources. For information, see the *IBM QRadar Administration Guide*.
Information > **Search Events**	Searches for events that are associated with this IP address.
Information > **Search Flows**	Searches for flows that are associated with this IP address.
Information > **Search Connections**	Searches for connections that are associated with this IP address. This option is only displayed if you purchased IBM QRadar Risk Manager and connected QRadar and the IBM QRadar Risk Manager appliance. For more information, see the *IBM QRadar Risk Manager User Guide*.
Information > **Switch Port Lookup**	Determines the switch port on a Cisco IOS device for this IP address. This option applies only to switches that are discovered by using the **Discover Devices** option on the **Risks** tab. **Note:** This menu option isn't available in QRadar Log Manager.
Information > **View Topology**	Displays the **Risks** tab, which depicts the layer 3 topology of your network. This option is available if you purchased IBM QRadar Risk Manager and connected QRadar and the IBM QRadar Risk Manager appliance.
Run Vulnerability Scan	Select the **Run Vulnerability Scan** option to scan an IBM QRadar Vulnerability Manager scan on this IP address. This option is only displayed when IBM QRadar Vulnerability Manager has been purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

System time

The upper right of the QRadar console displays the system time, which is the local 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 IBM

QRadar : QRadar User Guide

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** and **Network Activity** tabs, you must use the console system time to specify a time range.

Updating user preferences

You can set your preferences, such as locale, in IBM QRadar SIEM.

Procedure

1. Click the user icon, and then click **User Preferences** to access your user information.
2. Update your preferences.

Option	Description
Username	Displays your user name. You cannot edit this field.
Password	QRadar user passwords are stored as a salted SHA-256 string. The password must meet the minimum length and complexity requirements that are enforced.
Password (Confirm)	Password confirmation
Email Address	The email address must meet the following requirements: • Minimum of 10 characters • Maximum of 255 characters
Locale	QRadar is available in the following languages: English, Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, Italian, Spanish, Russian, and Portuguese (Brazil). If you choose a different language, the user interface is displayed in English. Other associated cultural conventions, such as character type, collation, format of date and time, and currency unit are used.
Enable Popup Notifications	If you want to enable pop-up system notifications to be displayed on your user interface, select this check box.

3. Click **Save**.

Chapter 3. Dashboard management

Use the **Dashboard** tab, which is the default view when you log into IBM QRadar, to focus on specific areas of your network security. The workspace supports multiple dashboards on which you can display your views of network security, activity, or data that is collected.

Tip: Use the QRadar Pulse app for an enhanced dashboard experience. The Pulse app is included with QRadar 7.4.0 and later. For more information about the Pulse app, see QRadar Pulse app (https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.Pulseapp.doc/c_Qapps_PulseDashboard_intro.html?cp=SS42VS_7.4).

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. For example, you can make these customizations:

- 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.

Default dashboards

Use the default dashboard to customize your items into functional views. These functional views focus on specific areas of your network.

The **Dashboard** tab provides five default dashboards that are focused on security, network activity, application activity, system monitoring, and compliance.

Each dashboard displays a default that is set of dashboard items. The dashboard items act as starting point to navigate to more detailed data. The following table defines the default dashboards.

Table 5. Default dashboards

Default dashboard	Items

Application Overview	The **Application Overview** dashboard includes the following default items: • Inbound Traffic by Country (Total Bytes) • Outbound Traffic by Country (Total Bytes) • Top Applications (Total Bytes) • Top Applications Inbound from Internet (TotalBytes) • Top Applications Outbound to the Internet (TotalBytes) • Top Services Denied through Firewalls (EventCount) • DSCP - Precedence (Total Bytes)

© Copyright IBM Corp. 2012, 2021

Table 5. Default dashboards (continued)	
Default dashboard	**Items**
Compliance Overview	The **Compliance Overview** dashboard includes the following default items: • Top Authentications by User (Time Series) • Top Authentication Failures by User (EventCount) • Login Failures by User (real-time) • Compliance: Username Involved in ComplianceRules (time series) • Compliance: Source IPs Involved in ComplianceRules (time series) • Most Recent Reports •
Network Overview	The **Network Overview** dashboard includes the following default items: • Top Talkers (real time) • ICMP Type/Code (Total Packets) • Top Networks by Traffic Volume (Total Bytes) • Firewall Deny by DST Port (Event Count) • Firewall Deny by DST IP (Event Count) • Firewall Deny by SRC IP (Event Count) • Top Applications (Total Bytes) • Link Utilization (real-time) • DSCP - Precedence (Total Bytes)
System Monitoring	The **System Monitoring** dashboard includes the following default items: • Top Log Sources (Event Count) • Link Utilization (real-time) • System Notifications • Event Processor Distribution (Event Count) • Event Rate (Events per Second Coalesced - Average 1 Min) • Flow Rate (Flows per Second - Peak 1 Min)
Table 5. Default dashboards (continued)	
Default dashboard	**Items**

Threat and Security Monitoring	The **Threat and Security Monitoring** dashboard includes the following default items: • Default-IDS/IPS-All: Top Alarm Signatures (real-time) • Top Systems Attacked (Event Count) • Top Systems Sourcing Attacks (Event Count) • My Offenses • Most Severe Offenses • Most Recent Offenses • Top Services Denied through Firewalls (EventCount) • Internet Threat Information Center • Flow Bias (Total Bytes) • Top Category Types • Top Sources • Top Local Destinations

Custom dashboards

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

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

- Create custom dashboards that are relevant to your responsibilities. 255 dashboards per user is themaximum; however, performance issues might occur if you create more than 10 dashboards.
- Add and remove dashboard items from default or custom dashboards.
- Move and position items to meet your requirements. When you position items, each item automaticallyresizes 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 **Network Activity** or **Log Activity** tabs 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.

Flow search

You can display a custom dashboard item that is based on saved search criteria from the **Network Activity** tab.

Flow search items are listed in the **Add Item** > **Network Activity** > **Flow Searches** menu. The name of the flow search item matches the name of the saved search criteria the item is based on.

Default saved search criteria is available and is preconfigured to display flow search items on your **Dashboard** tab menu. You can add more flow search dashboard items to your **Dashboard** tab menu. For more information, see Adding search-based dashboard items to the Add Items list.

On a flow search dashboard item, search results display real-time last-minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about configuring charts, see Configuring charts.

Time series charts are interactive. Using the time series charts, you can magnify and scan through a timeline to investigate network activity.

Offenses

You can add several offense-related items to your dashboard.

Note: Hidden or closed offenses are included in the values that are displayed in the **Dashboard** tab. For more information about hidden or closed events, see Offense management.

The following table describes the Offense items:

Table 6. Offense items

Dashboard items	**Description**
Most Recent Offenses	The five most recent offenses are identified with a magnitude bar to inform you of the importance of the offense. Point to the offense name to view detailed information for the IP address.
Most Severe Offenses	The five most severe offenses are identified with a magnitude bar to inform you of the importance of the offense. Point to the offense name to view detailed information for the IP address.
My Offenses	The **My Offenses** item displays 5 of the most recent offenses that are assigned to you. The offenses are identified with a magnitude bar to inform you of the importance of the offense. Point to the IP address to view detailed information for the IP address.
Top Sources	The **Top Sources** item displays the top offense sources. Each source is identified with a magnitude bar to inform you of the importance of the source. Point to the IP address to view detailed information for the IP address.
Top Local Destinations	The **Top Local Destinations** item displays the top local destinations. Each destination is identified with a magnitude bar to inform you of the importance of the destination. Point to the IP address to view detailed information for the IP
Categories	The **Top Categories Types** item displays the top 5 categories that are associated with the highest number of offenses.

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

Dashboard item	Description
Event Searches	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** > **Network Activity** > **Event Searches** menu. The name of the event search item matches the name of the saved search criteria the item is based on. QRadar 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.
Events By Severity	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.
Top Log Sources	The **Top Log Sources** dashboard item displays the top 5 log sources that sent events to QRadar 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.

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 Flows Per Second** - Displays the flow rate per second.
- **Flows (Past 24 Hours)** - Displays the total number of active flows that are seen within the last 24 hours.
- **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.
- **Updated Offenses (Past 24 Hours)** - Displays the total number of offenses that have been either created or modified with new evidence within the last 24 hours.
- **Data Reduction Ratio** - Displays the ratio of data reduced based on the total events that are detected within the last 24 hours and the number of modified offenses within the last 24 hours.

Risk Monitoring Dashboard

You use the **Risk Monitoring** dashboard to monitor policy risk and policy risk change for assets, policies and policy groups.

By default, the **Risk Monitoring** dashboard displays **Risk** and **Risk Change** items that monitor the policy risk score for assets in the High Vulnerabilities, Medium Vulnerabilities, and Low Vulnerabilities policy groups, as well as compliance pass rates and historical changes in policy risk score in the CIS policy group.

The Risk Monitoring dashboard items do not display any results unless IBM QRadar Risk Manager is licensed. For more information, see QRadar Risk Manager Users Guide.

To view the default **Risk Monitoring** dashboard, select **Show Dashboard** > **Risk Monitoring** on the **Dashboard** tab.

Related tasks

Monitoring policy compliance

Monitoring risk change

Monitoring policy compliance

Create a dashboard item that shows policy compliance pass rates and policy risk score for selected assets, policies, and policies groups.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a name and description for your policy compliance dashboard.
4. Click **OK**.
5. On the toolbar, select **Add Item** > **Risk Manager** > **Risk**.

   Risk Manager dashboard items are displayed only when IBM QRadar Risk Manager is licensed.
6. On the header of the new dashboard item, click the yellow **Settings** icon.
7. Use the **Chart Type**, **Display Top**, and **Sort** lists to configure the chart.
8. From the **Group** list, select the group that you want to monitor. For more information, see the table in step 9.

   When you select the **Asset** option, a link to the **Risks** > **Policy Management** > **By Asset** page appears at the bottom of the **Risk** dashboard item. The **By Asset** page displays more detailed information about all results that are returned for the selected **Policy Group**. For more information on a specific asset, select **Table** from **Chart Type** list and click the link in the **Asset** column to view details about the asset in the **By Asset** page.

   When you select the **Policy** option, a link to the **Risks** > **Policy Management** > **By Policy** page appears at the bottom of the **Risk** dashboard item. The **By Policy** page displays more detailed information about all results that are returned for the selected **Policy Group**. For more information on a specific policy, select **Table** from **Chart Type** list and click the link in the **Policy** column to view details about the policy in the **By Policy** page.
9. From the **Graph** list, select the graph type that you want to use. For more information, see the following table:

Group	**Asset Passed Percentage**	**Policy Checks Passed Percentage**	**Policy Group Passed Percentage**	**Policy Risk Score**
All	Returns the average asset percentage pass rate across assets, policies, and the policy group.	Returns the average policy check percentage pass rate across assets, policies, and the policy group.	Returns the average policy group pass rate across all assets, policies, and the policy group.	Returns the average policy risk score across all assets, policies, and the policy group.
Asset	Returns whether an asset passes asset compliance (100%=passed, 0%=failed). Use this setting to show which assets associated with a Policy Group pass compliance.	Returns percentage of policy checks that an asset passes. Use this setting to show the percentage of policy checks that passed for each asset that is associated with the Policy Group.	Returns the percentage of policy subgroups that are associated with the asset that pass compliance.	Returns the sum of all importance factor values for policy questions that are associated with each asset. Use this setting to view the policy risk for each asset that is associated with a selected policy group.

Policy	Returns whether all the assets associated with each policy in a Policy group pass compliance. Use this setting to monitor whether all the assets associated with each policy in a Policy Group pass or not.	Returns percentage of policy checks that pass per policy in the policy group. Use this setting to monitor how many policy checks are failing per policy.	Returns the percentage of policy subgroups of which the policy is a part that pass compliance.	Returns the importance factor values for each policy question in the Policy group. Use this setting to view the importance factor for each policy in a policy group.
Policy Group	Returns the percentage of assets that pass compliance for the selected Policy Group as a whole.	Returns the percentage of policy checks that pass per policy for the policy group as a whole.	Returns the percentage of policy subgroups within the Policy Group that pass compliance.	Returns the sum of all importance factor values for all policy questions in the Policy group.

10. From the **Policy Group** list, select the policy groups that you want to monitor.
11. Click **Save**.

Monitoring risk change

Create a dashboard item that shows policy risk change for selected assets, policies, and policies groups on a daily, weekly, and monthly basis.

About this task

Use this dashboard item to compare changes in the Policy Risk Score, Policies Checks, and Policies values for a policy group over time.

The **Risk Change** dashboard item uses arrows to indicate where policy risk for selected values that increased, decreased, or stayed the same over a chosen time period:

- The number beneath the red arrow indicates the values that show an increased risk.
- The number beneath the gray arrows indicates the values where there is no change in risk.
- The number beneath the green arrow indicates the values that show a decreased risk.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a name and description for your historical policy compliance dashboard.
4. Click **OK**.
5. On the toolbar, select **Add Item** > **Risk Manager** > **Risk Change**.

   Risk Manager Dashboard items are displayed only when IBM QRadar Risk Manager is licensed.
6. On the header of the new dashboard item, click the yellow **Settings** icon.
7. From the **Policy Group** list, select the policy groups that you want to monitor.
8. Select an option from the **Value To Compare** list:
   - If you want to see the cumulative changes in importance factor for all policy questions within the selected policy groups, select **Policy Risk Score**.

- If you want to see how many policy checks changed within the selected policy groups, select **Policies Checks**.
- If you want to see how many policies changed within the selected policy groups, select **Policies**.

9. Select the risk change period that you want to monitor from the **Delta Time** list:
   - If you want to compare risk changes from 12:00 a.m. today with yesterday's risk changes, select **Day**.
   - If you want to compare risk changes from Monday 12:00 a.m. this week with last week's risk changes, select **Week**.
   - If you want to compare risk changes from the 12:00 a.m. on the first day of the current month with last month's risk changes, select **Month**.
10. Click **Save**.

Vulnerability Management items

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

For more information, see the *IBM 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 QRadar 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.

Creating a custom dashboard

You can create a custom dashboard to view a group of dashboard items that meet a particular requirement.

About this task

After you create a custom dashboard, the new dashboard is displayed in the **Dashboard** tab and is listed in the **Show Dashboard** list box. A new custom dashboard is empty by default; therefore, you must add items to the dashboard.

Procedure

1. Click the **Dashboard** tab.
2. Click the **New Dashboard** icon.
3. In the **Name** field, type a unique name for the dashboard. The maximum length is 65 characters.
4. In the **Description** field, type a description of the dashboard. The maximum length is 1024 characters. This description is displayed in the tooltip for the dashboard name in the **Show Dashboard** list box.
5. Click **OK**.

Using the dashboard to investigate log or network activity

Search-based dashboard items provide a link to the **Log Activity** or **Network Activity** tabs, allowing you to further investigate log or network 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.

To investigate flows from a **Network Activity** dashboard item:

1. Click the **View in Network Activity** link. The **Network 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** or **Network Activity** tab depend on which chart is configured in the dashboard item:

Chart type	Description
Bar, Pie, and Table	The **Log Activity** or **Network Activity** tab displays a bar chart, pie chart, and table of flow details.

Time Series	The **Log Activity** or **Network 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 atable of event or flow details are displayed. 2. If your time range is more than 1 hour, a time series chart is displayed and you areprompted to click Update Details. This action starts the search that populates the event or flow details and generates the bar chart. When the search completes, the bar chart and table of event or flow details are displayed.

Configuring dashboard chart types

You can configure different dashboard chart types for presenting your organization's data in meaningful ways.

Alternatively, use the IBM QRadar Pulse dashboard app to communicate insights and analysis about your network. Visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, a built-in 3D threat globe, and auto updating charts. For more information, see QRadar Pulse app (https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm/Pulseapp.doc/c_Qapps_PulseDashboard_intro.html).

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.
   a) From the **Value to Graph** list box, select the object type that you want to graph on the chart. Options include all normalized and custom event or flow parameters that are included in your search parameters.
   b) Select a chart type:
      - Bar, pie, and table charts are only available for grouped events or flows.
      - Data accumulates so that when you run a time series saved search, a cache of event or flowsdata is 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.

        Select the **Capture Time Series Data** checkbox to enable time series capture. When you select this checkbox, the chart feature accumulates data for time series charts. By default, this option is disabled.

Results

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

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 inseparate 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**.

What to do next

To delete a dashboard of another user, see Deleting a user account in QRadar and reassignment of dependents.

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

Procedure

1. Choose:
   - To add a flow search dashboard item, click the **Network Activity** tab.
   - 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 tothe **Add Items** list
   a) Click the **Dashboard** tab.
   b) Choose one of the following options:
   a) To verify an event search item, select **Add Item** > **Log Activity** > **Event Searches** > **Add Item**.
   b) To verify a flow search item, select **Add Item** > **Network Activity** > **Flow Searches**.

The dashboard item is displayed on the list with the same name as your saved search criteria.

Chapter 4. Offense management

IBM QRadar reduces billions of events and flows into a manageable number of actionable offenses that are prioritized by their impact on your business operations. Use the **Offenses** tab to access all of the data that you need to understand even the most complex threats.

By providing immediate context for the offense, QRadar helps you to quickly identify which offenses are the most important, and to begin an investigation to find the source of the suspected security attack or policy breach.

Tip: You can also manage offenses using the IBM QRadar Analyst Workflow interface. For more information, see Chapter 5, "QRadar Analyst Workflow," on page 45.

Restriction: You cannot manage offenses in IBM QRadar Log Manager. For more information about the differences between IBM QRadar SIEM and IBM QRadar Log Manager, see Chapter 2, "Capabilities in your IBM QRadar product," on page 5.

Offense prioritization

The magnitude rating of an offense is a measure of the importance of the offense in your environment. IBM QRadar uses the magnitude rating to prioritize offenses and help you to determine which offenses to investigate first.

The *magnitude rating* of an offense is calculated based on relevance, severity, and credibility.

- *Relevance* determines the impact of the offense on your network. For example, if a port is open, the relevance is high.
- *Credibility* indicates the integrity of the offense as determined by the credibility rating that is configured in the log source. Credibility increases as multiple sources report the same event.
- *Severity* indicates the level of threat that a source poses in relation to how prepared the destination is for the attack.

QRadar uses complex algorithms to calculate the offense magnitude rating, and the rating is re-evaluated when new events are added to the offense and also at scheduled intervals. The following information is considered when the offense magnitude is calculated:

- the number of events and flows that are associated with the offense
- the number of log sources
- the age of the offense
- the weight of the assets associated with the offense
- the categories, severity, relevance, and credibility of the events and flows that contribute to the offense
- the vulnerabilities and threat assessment of the hosts that are involved in the offense

The magnitude rating of an offense is different from the magnitude rating for an event. You can influence the magnitude of an offense by setting the event magnitude in the rule actions, but you cannot bypass the QRadar algorithms to set the offense magnitude yourself.

Offense chaining

IBM QRadar chains offenses together to reduce the number of offenses that you need to review, which reduces the time to investigate and remediate the threat.

Offense chaining helps you find the root cause of a problem by connecting multiple symptoms together and showing them in a single offense. By understanding how an offense changed over time, you can see things that might be overlooked during your analysis. Some events that would not be worth investigating on their own might suddenly be of interest when they are correlated with other events to show a pattern. © Copyright IBM Corp. 2012, 2021

Offense chaining is based on the offense index field that is specified on the rule. For example, if your rule is configured to use the source IP address as the offense index field, there is only one offense that has that source IP address for while the offense is active.

You can identify a chained offense by looking for preceded by in the **Description** field on the **Offense Summary** page. In the following example, QRadar combined all of the events that fired for each of the three rules into one offense, and appended the rule names to the **Description** field:

```
Exploit Followed By Suspicious Host Activity - Chained
preceded by Local UDP Scanner Detected preceded by XForce Communication to a known Bot Command and
Control
```

Offense indexing

Offense indexing provides the capability to group events or flows from different rules indexed on the same property together in a single offense.

IBM QRadar uses the offense index parameter to determine which offenses to chain together. For example, an offense that has only one source IP address and multiple destination IP addresses indicates that the threat has a single attacker and multiple victims. If you index this type of offense by the source IP address, all events and flows that originate from the same IP address are added to the same offense.

You can configure rules to index an offense based on any piece of information. QRadar includes a set of predefined, normalized fields that you can use to index your offenses. If the field that you want to index on is not included in the normalized fields, create a custom event or a custom flow property to extract the data from the payload and use it as the offense indexing field in your rule. The custom property that you index on can be based on a regular expression, a calculation, or an AQL-based expression.

Offense indexing considerations

It is important to understand how offense indexing impacts your IBM QRadar deployment.

System performance

Ensure that you optimize and enable all custom properties that are used for offense indexing. Using properties that are not optimized can have a negative impact on performance.

When you create a rule, you cannot select non-optimized properties in the **Index offense based on** field. However, if an existing rule is indexed on a custom property, and then the custom property is de-optimized, the property is still available in the offense index list. Do not de-optimize custom properties that are used in rules.

Rule action and response

When the indexed property value is null, an offense is not created, even when you select the **Ensure the detected event is part of an offense** check box in the rule action. For example, if a rule is configured to create an offense that is indexed by host name, but the host name in the event is empty, an offense is not created even though all of the conditions in the rule tests are met.

When the response limiter uses a custom property, and the custom property value is null, the limit is applied to the null value. For example, if the response is **Email**, and the limiter says **Respond no more than 1 time per 1 hour per custom property**, if the rule fires a second time with a null property within 1 hour, an email will not be sent.

When you index using a custom property, the properties that you can use in the rule index and response limiter field depends on the type of rule that you are creating. An event rule accepts custom event properties in the rule index and response limiter fields, while a flow rule accepts only custom flow properties. A common rule accepts either custom event or custom flow properties in the rule index and response limiter fields.

You cannot use custom properties to index an offense that is created by a dispatched event.

Payload contents

Offenses that are indexed by the Ariel Query Language (AQL), a regular expression (regex), or by a calculated property include the same payload as the initial event that generated the offense.

Offenses that are indexed by a normalized event field, such as Source IP or Destination IP, include the event name and description as the custom rules engine (CRE) payload.

Example: Detecting malware outbreaks based on the MD5 signature

As a network security analyst for a large organization, you use QRadar to detect when a malware outbreak occurs. You set the criteria for an outbreak as a threat that occurs across 10 hosts within 4 hours. You want to use the MD5 signature as the basis for this threat detection.

You configure IBM QRadar to evaluate the incoming logs to determine whether a threat exists, and then you group all of the fired rules that contain the same MD5 signature into a single offense.

1. Create a custom property to extract the MD5 signature from the logs. Ensure that the custom property is optimized and enabled.
2. Create a rule and configure the rule to create an offense that uses the MD5 signature custom property as the offense index field. When the rule fires, an offense is created. All fired rules that have the same MD5 signature are grouped into one offense.
3. You can search by offense type to find the offenses that are indexed by the MD5 signature custom property.

Offense retention

The state of an offense determines how long IBM QRadar keeps the offense in the system. The offense retention period determines how long inactive and closed offenses are kept before they are removed from the QRadar console.

Active offenses

When a rule triggers an offense, the offense is active. In this state, QRadar is waiting to evaluate new events or flows against the offense rule test. When new events are evaluated, the offense clock is reset to keep the offense active for another 30 minutes.

Dormant offenses

An offense becomes dormant if new events or flows are not added to the offense within 30 minutes, or if QRadar did not process any events within 4 hours. An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the five-day counter is reset.

Inactive offenses

An offense becomes inactive after 5 days in a dormant state. In the inactive state, new events that trigger the offense rule test do not contribute to the inactive offense. They are added to a new offense.

Inactive offenses are removed after the offense retention period elapses.

Closed offenses

Closed offenses are removed after the offense retention period elapses. If more events occur for an offense that is closed, a new offense is created.

If you include closed offenses in a search, and the offense wasn't removed from the QRadar console, the offense is displayed in the search results.

The default offense retention period is 30 days. After the offense retention period expires, closed and inactive offenses are removed from the system. Offenses that are not inactive or closed are retained indefinitely.

Important: System performance is negatively impacted when the system retains many inactive and closed offenses. For optimum performance, set the retention period for the least amount of time possible. The suggested retention period is 3 days.

To prevent an offense from being removed from the system, you can protect it. Before you protect offenses, consider the performance impact that it might have. Some offenses impact system performance more than others. For example, offenses with large numbers of events and flows have a greater impact on performance. Offenses that have many targets and destinations impact performance more than an offense that has only a single target or destination.

If you need to re-create an offense after it is removed from the system, run a historical correlation job to analyze the historical data. For more information, see Chapter 13, "Historical correlation," on page 203.

Protecting offenses

You might have offenses that you want to retain regardless of the retention period. You can protect offenses to prevent them from being removed from QRadar after the retention period has elapsed.

About this task

By default, offenses are retained for thirty days. For more information about customizing the offense retention period, see the *IBM QRadar Administration Guide*.

Procedure

1. Click the **Offenses** tab, and click **All Offenses**.
2. Choose one of the following options:
   - Select the offense that you want to protect, and then select **Protect** from the **Actions** list.
   - From the **Actions** list box, select **Protect Listed**.
3. Click **OK**.

Results

The offense is protected and will not be removed from QRadar. In the **Offense** window, the protected offense is indicated by a **Protected** icon in the Flag column.

Unprotecting offenses

You can unprotect offenses that were previously protected from removal after the offense retention period has elapsed.

About this task

To list only protected offenses, you can perform a search that filters for only protected offenses. If you clear the **Protected** check box and ensure that all other options are selected under the **Excludes option** list on the Search Parameters pane, only protected offenses are displayed.

Procedure

1. Click the **Offenses** tab.

2. Click **All Offenses**.
3. Optional: Perform a search that displays only protected offenses.
4. Choose one of the following options:
   - Select the offense that you no longer want to protect, and then select **Unprotect** from the Actions list box.
   - From the **Actions** list box, select **Unprotect Listed**.
5. Click **OK**.

Offense investigations

IBM QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step; identifying how it happened, where it happened, and who did it requires some investigation.

The **Offense Summary** window helps you begin your offense investigation by providing context to help you understand what happened and determine how to isolate and resolve the problem.

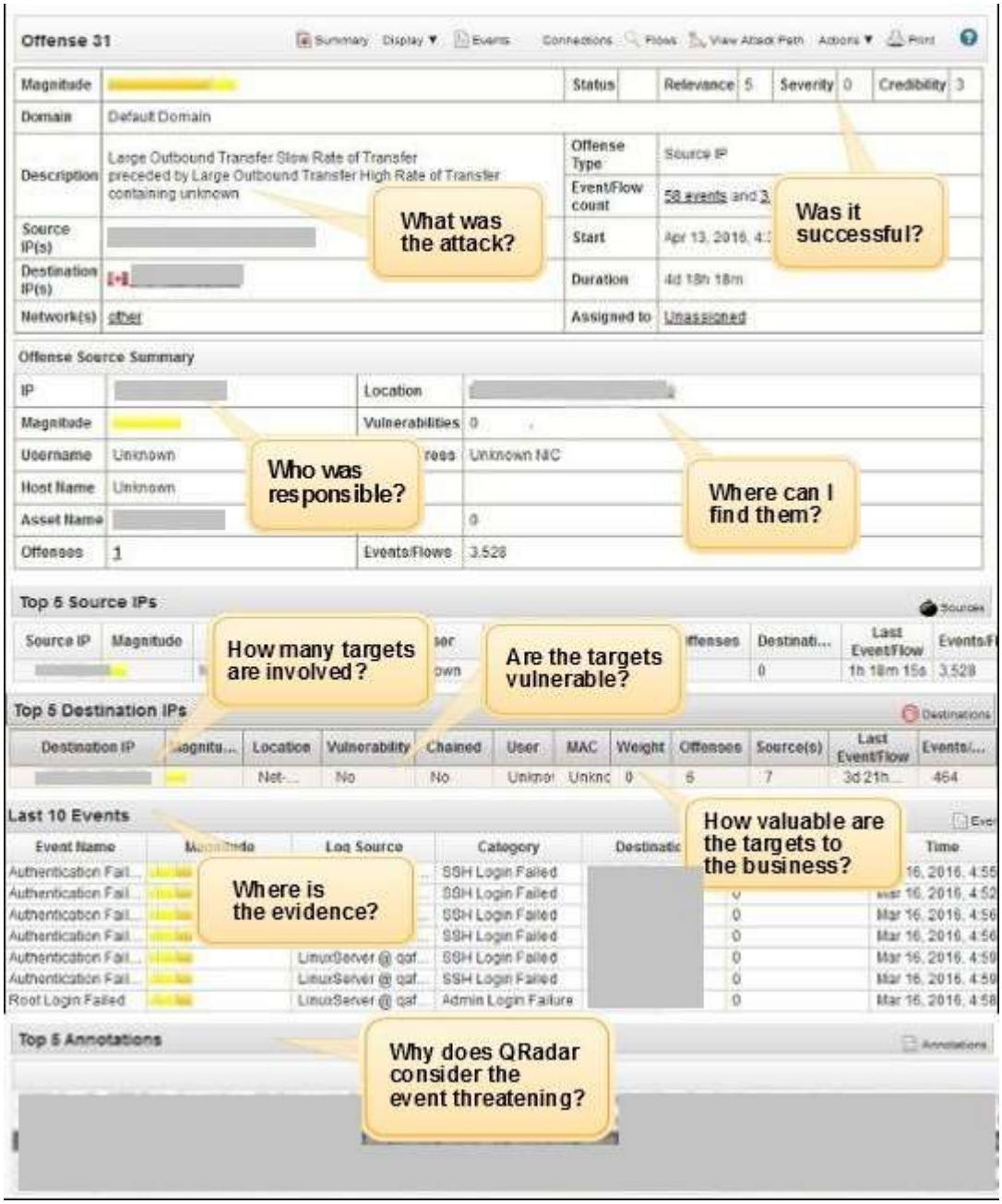


Figure 3. Offense Summary view

QRadar does not use device level user permissions to determine which offenses each user is able to view. All users who have access to the network can view all offenses regardless of which log source or flow source is associated with the offense. For more information about restricting network access, see the security profiles documentation in the *IBM QRadar Administration Guide*.

Selecting an offense to investigate

The **Offenses** tab shows the suspected security attacks and policy breaches that are occurring on your network. Offenses are listed with the highest magnitude first. Investigate the offenses at the top of the list first.

About this task

Use the navigation options on the left to view the offenses from different perspectives. For example, select **By Source IP** or **By Destination IP** to view information about repeat offenders, IP addresses that generate many attacks, or systems that are continually under attack. You can further refine the offenses in the list by selecting a time period for the offenses that you want to view or by changing the search parameters.

You can also search for offenses that are based on various criteria. For more information about searching offenses, see "Offense searches" on page 154.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, select the category of offenses that you want to view.
3. Depending on the category that you selected, you may be able to select the following filtering options:
   a) From the **View Offenses** list, select an option to filter the list of offenses for a specific time frame.
   b) In the **Current Search Parameters** pane, click **Clear Filter** links to refine the list of offenses.
4. To view all global offenses that are occurring on the network, click **All Offenses**.
5. To view all offenses that are assigned to you, click **My Offenses**.
6. To view offenses grouped on the high-level category, click **By Category**.
   a) To view low-level category groups for a particular high-level category, click the arrow icon next tothe high-level category name.
   b) To view a list of offenses for a low-level category, double-click the low-level category.

      Count fields, such as **Event/Flow Count** and **Source Count** do not consider the network permissions of the user.
7. To view offenses grouped by source IP address, click **By Source IP**.

   The list of offenses displays only source IP addresses with active offenses.
   a) Double-click the **Source IP** group that you want to view.
   b) To view a list of local destination IP addresses for the source IP address, click **Destinations** on the **Source** page toolbar.
   c) To view a list of offenses that are associated with this source IP address, click **Offenses** on the **Source** page toolbar.
8. To view offenses grouped by destination IP address, click **By Destination IP**.
   a) Double-click the **Source IP** address group that you want to view.
   b) To view a list of offenses that are associated with the destination IP address, click **Offenses** on the **Destination** page toolbar.
   c) To view a list of source IP addresses associated with the destination IP address, click **Sources** on the **Destination** page toolbar.
9. To view offenses grouped by network, click **By Network**.
   a) Double-click the **Network** that you want to view.
   b) To view a list of source IP addresses associated with this network, click **Sources** on the **Network** page toolbar.
   c) To view a list of destination IP addresses associated with this network, click **Destinations** on the **Network** page toolbar.
   d) To view a list of offenses that are associated with this network, click **Offenses** on the **Network** page toolbar.
10. Double-click the offense to see additional information.

What to do next

Use the information in the offense summary and details to investigate the offense and take necessary actions.

Investigating an offense by using the summary information

The **Offense Summary** window provides the information that you need to investigate an offense in IBM QRadar. The information that is most important to you during your investigation might be different, depending on the type of offense that you are investigating.

To make it easier for you to investigate an offense, the bottom of the **Offense Summary** page groups information about top contributors to the offense. These fields show only the most recent or most important pieces of information in that category. Many fields show more information when you hover the mouse over them. Some fields have right-click menu options.

Procedure

1. Click the **Offenses** tab and double-click the offense that you want to investigate.
   The **Offense Summary** window opens.
2. Review the first row of data to learn about the level of importance that QRadar assigned to the offense.

   Learn more about the magnitude rating:

Parameter	Description
Magnitude	Indicates the relative importance of the offense. This value is calculated based on the relevance, severity, and credibility ratings.
Status	Hover your mouse over the status icon to see the status. QRadar does not display a status icon when an offense is active.
Relevance	Indicates the importance of the destination. QRadar determines the relevance by the weight that the administrator assigned to the networks and assets.
Severity	Indicates the threat that an attack poses in relation to how prepared the destination is for the attack.
Credibility	Indicates the integrity of the offense as determined by the credibility rating that is configured in the log source. Credibility increases as multiple sources report the same event. QRadar administrators configure the credibility rating of log sources.

3. Review the information in the top portion of the **Offense Summary** window to learn more about the type of attack and the timeframe when it occurred.

   Learn more about the offense information:

Parameter	Description
Description	Shows the cause of the offense.
Parameter	**Description**

	Chained offenses show **Preceded by**, indicating that the offense changed over time as new events and flows were added to offense.
Offense Type	The offense type is determined by the rule that created the offense. The offense type determines what type of information is displayed in the **Offense Source Summary** pane.
Event/Flow count	To see the list of events and flows that contributed to the offense, click the **Event** or **Flow** links. If the flow count displays **N/A**, the offense might have a start date that precedes the date when you upgraded to IBM QRadar version 7.1 (MR1). The flows cannot be counted, but you can click the **N/A** link to investigate the flows.
Source IP(s)	Specifies the device that attempts to breach the security of a component on your network. The device can have an IPv4 or IPv6 address. Offenses of type **Source IP** always originate from only one source IP address. Offenses of other types can have more than one source IP address. You can see more information about the source IP address by hovering the mouse over the address, or by using right-click and left-click mouse actions.
Destination IP(s)	Specifies the network device that the source IP address attempted to access. The network device can have an IPv4 or IPv6 address. If the offense has only one target, the IP address is displayed. If the offense has multiple targets, the number of local or remote IP addresses that were targeted. You can see more information by hovering the mouse over the address, or by using right-click and left-click mouse actions.
Start	Specifies the date and time when the first event or flow occurred for the offense.
Duration	Specifies the amount of time that elapsed since the first event or flow that is associated with the offense was created.
Network(s)	Specifies the local networks of the local destination IP addresses that were targeted. QRadar considers all networks that are specified in the network hierarchy as local. The system does not associate remote networks to an offense, even if they are specified as a remote network or a remote service on the **Admin** tab.

4. In the **Offense Source Summary** window, review the information about the source of the offense.

   The information that is shown in the **Offense Source Summary** window depends on the **Offense Type** field.

   Learn more about the source summary information:

Parameter	**Description**

Chained	Specifies whether the destination IP address is chained. A chained IP address is associated with other offenses. For example, a destination IP address might become the source IP address for another offense. If the destination IP address is chained, click **Yes** to view the chained offenses.
Parameter	**Description**
Destination IP(s)	Specifies the network device that the source IP address attempted to access. The network device can have an IPv4 or IPv6 address. If the offense has only one target, the IP address is displayed. If the offense has multiple targets, this field shows the number of local or remote IP addresses that were targeted. You can see more information by hovering the mouse over the address, or by using right-click and left-click mouse actions.
Location	Specifies the network location of the source or destination IP address. If the location is local, click the link to view the networks.
Magnitude	Specifies the relative importance of the source or destination IP address. The magnitude bar provides a visual representation of the CVSS risk value of the asset that is associated with the IP address. Hover your mouse over the magnitude bar to display the calculated magnitude.
Severity	Specifies the severity of the event or offense. Severity specifies the level of threat that an offense poses in relation to how prepared the destination IP address is for the attack. This value is directly mapped to the event category that correlates to the offense. For example, a Denial of Service (DoS) attack has a severity of 10, which specifies a severe occurrence.
Source IP(s)	Specifies the device that attempted to breach the security of a component on your network. The device can have an IPv4 or IPv6 address. Offenses of type **Source IP** always originate from only one source IP address. Offenses of other types can have more than one source IP address. You can see more information about the source IP address by hovering the mouse over the address, or by using right-click and left-click mouse actions.
Username	Specifies the user name that is associated with the event or flow that created the offense. Hover your mouse over the user name to see the most recent information in the asset model database for the user. Events that do not include a user name in the payload, or system-generated events that belong to a local computer or a system account, show Unknown. To access more information that is associated with a selected user name, right-click the user name for **View Assets** and **View Events** menu options.
Vulnerabilities	Specifies the number of identified vulnerabilities that are associated with the source or destination IP address. This value also includes the number of active and passive vulnerabilities.

When you view the summary information for historical offenses, the **Last Known** data fields are not populated.

5. In the bottom portion of the **Offense Summary** window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense. To see all the information that QRadar collected in a category, click the links on the right side of the category heading.

Learn more about the information presented in the offense details:

Offense details category	Description
Last 5 Notes	Use notes to track important information that is gathered during the offense investigation. You can add a note to an offense, but you cannot edit or delete notes.
Top 5 Source IPs	Shows the top 5 IP addresses with the highest magnitude, which is where the suspected attack or policy breach originated. Offenses that have only one source IP address show only one entry in the table.
Top 5 Destination IPs	Shows the top 5 local IP addresses with the highest magnitude, which might indicate the target of the attack. Offenses that target less than 5 local IP addresses show fewer entries in the table. The **Chained** column indicates whether the destination IP address is the source IP address of another offense. A **Yes** in this column indicates that an attacker has control over the system with this IP address and is using it to attack other systems. The **Magnitude** column shows the aggregate Common Vulnerability Scoring System (CVSS) score when it exists. When no CVSS score is available, the column shows the highest magnitude of all the offenses that the IP address is a part of. When you hover the mouse over the destination IP address, the **Destination Magnitude** shows the CVSS score. When no CVSS score is available, a zero is displayed.
Top 5 Log Sources	Shows the log sources that contribute the most events to the offense. The Custom Rule Engine (CRE) creates an event and adds it to the offense when the test criteria that is specified in the custom rule matches the incoming event. A log source that displays **Custom Rule Engine** in the **Description** field indicates that QRadar created the events from that log source. **Total Events** shows the sum of all the events that are received from this log source while the offense was active.
Top 5 Users	Events must include user information in order for QRadar to populate this table.

Top 5 Categories	Shows the low-level categories that have the most events that contributed to the offense. **Local Destination Count** shows the number of local destination IP addresses affected by offenses with events in the category. When all destination IP addresses are remote, this field shows 0.
Last 10 Events	Shows information about the last 10 events that contributed to the offense.
Last 10 Flows	Shows information about the last 10 flows that contributed to the offense. The **Total Bytes** column shows the sum of the bytes transferred in both directions.
Annotations	Annotations provide insight into why QRadar considers the event or observed traffic to be threatening.
Offense details category	**Description**
	QRadar can add annotations when it adds events or flows to an offense. The oldest annotation shows information that QRadar added when the offense was created. Users cannot add, edit, or delete annotations.
Last 5 Search Results	Shows information about the results from the last five scheduled searches.

6. If you installed IBM QRadar Risk Manager, click **View Attack Path** to see which assets in your network are communicating to allow an offense to travel through the network.

Investigating events

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. Events that are associated with an offense provide evidence that suspicious activity is happening on your network. By examining the event data, you can understand what caused the offense and determine how best to isolate and mitigate the threat.

About this task

Some events are created based on an incoming raw event, while others are created by the QRadar Custom Rule Engine (CRE). Events that are created by QRadar do not have a payload because they are not based on raw events.

Procedure

1. In the **Offense Summary** window, click **Events**.

   The **List of Events** window shows all events that are associated with the offense.
2. Specify the **Start Time**, **End Time**, and **View** options to view events that occurred within a specific time frame.
3. Click the event column header to sort the event list.
4. In the list of events, right-click the event name to apply quick filter options to reduce the number of events to review.

   You can apply quick filters to other columns in the event list as well.

5. Double-click an event to view the event details.

   The **Event Information** and the **Source and Destination Information** window show only the information that is known about the event. Depending on the type of event, some fields might be empty.

   Learn more about the time fields on the Event Information:

Field	Description
Start Time	The time that QRadar received the raw event from the log source.
Storage Time	The time that QRadar stored the normalized event.
Log Source Time	The time that is recorded in the raw event from the log source.

6. In the **Payload Information** box, review the raw event for information that QRadar did not normalize.

   Information that is not normalized does not appear in the QRadar interface, but it may be valuable to your investigation.

What to do next

For more information about how to use QRadar to review event data, see "Log activity monitoring" on page 59 and Chapter 10, "Event and flow searches," on page 139.

Related information

QRadar: Event details and the difference between Start Time, Storage Time, and Log Source Time

Investigating flows

IBM QRadar correlates flows into an offense when it identifies suspicious activity in network communications. The flow analysis provides visibility into layer 7, or the application layer, for applications such as web browsers, NFS, SNMP, Telnet, and FTP. A flow can include information such as IP addresses, ports, applications, traffic statistics, and packet payload from unencrypted traffic.

By default, QRadar tries to extract normalized fields and custom flow properties from the first 64 bytes of flow data, but administrators can increase the content capture length to collect more data. For more information, see the *IBM QRadar Administration Guide*.

Procedure

1. In the **Offense Summary** window, click **Flows** in the upper right menu.

   The **Flow List** window shows all flows that are associated with the offense.
2. Specify the **Start Time**, **End Time**, and **View** options to view flows that occurred within a specific time frame.
3. Click the flow column header to sort the flow list.
4. In the list of flows, right-click the flow name to apply quick filter options to reduce the number of flows to review.

   You can apply quick filters to other columns in the flow list as well.
5. Double-click a flow to review the flow details.

   Learn more about the flow details:

Field	Description

Event Description	When the application is not identified in the payload, QRadar uses builtin decoding to determine the application, and shows Application detected with state-based decoding in **Event Description**.
Source Payload and **Destination Payload**	Shows the size of the payload. When the size exceeds 64 bytes, the payload might contain additional information that is not shown in the QRadar interface.
Custom Rules Partially Matched	Shows rules for which the threshold value was not met, but otherwise the rule matched.
Flow Direction	Specifies the flow direction, where L indicates local network, and R indicates remote network.

What to do next

For more information about how to use QRadar to review flow data, see Chapter 7, "Network activity monitoring," on page 79 and Chapter 10, "Event and flow searches," on page 139.

Offense actions

IBM QRadar provides the capability to act on the offenses as you investigate them. To help you track offenses that were acted upon, QRadar adds an icon to the **Flag** column when you assign an offense to a user, protect or hide an offense, add notes, or mark the offense for follow-up.

To perform the same action on multiple offenses, hold the Control key while you select each offense you want to act on. To view offense details on a new page, press the Ctrl key while you double-click an offense.

Adding notes

Add notes to an offense to track information that is collected during an investigation. Notes can include up to 2000 characters.

Procedure

1. Click the **Offenses** tab.
2. Select the offense to which you want to add the note.
   To add the same note to multiple offenses, press the Ctrl key while you select each offense.
3. From the **Actions** list, select **Add Note**.
4. Type the note that you want to include for this offense.
5. Click **Add Note**.

Results

The note is displayed in the **Last 5 Notes** pane on the **Offense Summary** window. A **Notes** icon is displayed in the flag column of the offense list.

Hover your mouse over the notes indicator in the **Flag** column of the **Offenses** list to view the note.

Hiding offenses

Hide an offense to prevent it from being displayed in the offense list. After you hide an offense, the offense is no longer displayed in any list on the **Offenses** tab, including the **All Offenses** list. However, if you perform a search that includes hidden offenses, the offense is displayed in the search results.

Procedure

1. Click the **Offenses** tab.
2. Select the offense that you want to hide.
   To hide multiple offenses, hold the Control key while you select each offense.
3. From the **Actions** list box, select **Hide**.
4. Click **OK**.

Showing hidden offenses

By default, the offense list on the **Offenses** tab filters to exclude hidden offenses. To view hidden offenses, clear the filter on the **Offenses** tab or perform a search that includes hidden offenses. When you include hidden offenses in the offense list, the offenses show the **Hidden** icon in the **Flag** column.

Procedure

1. Click the **Offenses** tab.
2. To clear the filter on the offense list, click **Clear Filter** next to the **Exclude Hidden Offenses** search parameter.
3. To create a new search that includes hidden offenses, follow these steps:
   a) From the **Search** list box, select **New Search**.
   b) In the **Search Parameters** window, clear the **Hidden Offenses** check box in the **Exclude** options list.
   c) Click **Search**.
4. To remove the hidden flag from an offense, follow these steps:
   a) Select the offense for which you want to remove the hidden flag.
      To select multiple offenses, hold the Control key while you click each offense.
   b) From the **Actions** list box, select **Show**.

   The hidden flag is removed and the offense appears in the offense list without having to clear the **Exclude Hidden Offenses** filter.

Closing offenses

Close an offense to remove it completely from your system.

About this task

The default offense retention period is 30 days. After the offense retention period expires, closed offenses are deleted from the system. You can protect an offense to prevent it from being deleted when the retention period expires.

Closed offenses are no longer displayed in any list on the **Offenses** tab, including the **All Offenses** list. If you include closed offenses in a search, and the offense is still within the retention period, the offense is displayed in the search results. If more events occur for an offense that is closed, a new offense is created.

When you close offenses, you must select a reason for closing the offense. If you have the **Manage Offense Closing** permission, you can add custom closing reasons. For more information about user role permissions, see the *IBM QRadar Administration Guide*.

Procedure

1. Click the **Offenses** tab.
2. Select the offense that you want to close.

   To close multiple offenses, hold the Control key while you select each offense.
3. From the **Actions** list, select **Close**.
4. In the **Reason for Closing** list, specify a closing reason.

   To add a close reason, click the icon beside **Reason for Closing** to open the **Custom Offense Close Reasons** dialog box.
5. In the **Notes** field, type a note to provide more information.

   The **Notes** field displays the note that was entered for the previous offense closing. Notes must not exceed 2,000 characters.
6. Click **OK**.

Results

After you close offenses, the counts that are displayed on the **By Category** window of the **Offenses** tab can take several minutes to reflect the closed offenses.

Exporting offenses

Export offenses when you want to reuse the data or when you want to store the data externally. For example, you can use the offense data to create reports in a third-party application. You can also export offenses as a secondary long-term retention strategy. Customer Support might require you to export offenses for troubleshooting purposes.

You can export offenses in Extensible Markup Language (XML) or comma-separated values (CSV) format. The resulting XML or CSV file includes the parameters that are specified in the **Column Definition** pane of the search parameters. The length of time that is required to export the data depends on the number of parameters specified.

Procedure

1. Click the **Offenses** tab.
2. Select the offenses that you want to export.

   To select multiple offenses, hold the Control key while you select each offense.
3. Choose one of the following options:
   - To export the offenses in XML format, select **Actions** > **Export to XML**.
   - To export the offenses in CSV format, select **Actions** > **Export to CSV**

     Note: If you use Microsoft Excel to import the CSV file, you must select the correct locale to ensure that the data displays correctly.

     .
4. Choose one of the following options:
   - To open the file for immediate viewing, select **Open with** and select an application from the list.

- To save the file, select **Save File**.

5. Click **OK**.

   The file, <*date*>-data_export.xml.zip, is saved in the default download folder on your computer.

Assigning offenses to users

By default, all new offenses are unassigned. You can assign an offense to an IBM QRadar user for investigation.

About this task

When you assign an offense to a user, the offense is displayed on the **My Offenses** page for that user. You must have the **Assign Offenses to Users** permission to assign offenses to users. For more information about user role permissions, see the *IBM QRadar Administration Guide*.

You can assign offenses to users from either the **Offenses** tab or **Offense Summary** pages. This procedure provides instruction on how to assign offenses from the **Offenses** tab.

Procedure

1. Click the **Offenses** tab.
2. Select the offense that you want to assign.

   To assign multiple offenses, hold the Control key while you select each offense.
3. From the **Actions** list, select **Assign**.
4. In the **Assign To User** list, select the user that you want to assign this offense to.

   Note: The **Assign To User** list displays only those users who have privileges to view the **Offenses** tab. The security profile settings for the user are followed as well.
5. Click **Save**.

Results

The offense is assigned to the selected user. The **User** icon is displayed in the Flag column of the **Offenses** tab to indicate that the offense is assigned. The designated user can see this offense on the **My Offenses** page.

Sending email notifications

Share the offense summary information with another person by sending an email.

The body of the email message includes the following information, if available:

- Source IP address
- Source user name, host name, or asset name
- Total number of sources
- Top five sources by magnitude
- Source networks
- Destination IP address
- Destination user name, host name, or asset name
- Total number of destinations
- Top five destinations by magnitude
- Destination networks
- Total number of events

- Rules that caused the offense or event rule to fire
- Full description of the offense or event rule
- Offense ID
- Top five categories
- Start time of the offense or the time the event was generated
- Top five annotations
- Link to the offense user interface
- Contributing CRE rules

Procedure

1. Click the **Offenses** tab.
2. Select the offense for which you want to send an email notification.
3. From the **Actions** list box, select **Email**.
4. Configure the following parameters:

Option	Description
Parameter	Description
To	Type the email address of the user you want to notify when a change occurs to the selected offense. Separate multiple email addresses with a comma.
From	Type the originating email address. The default is root@localhost.com.
Email Subject	Type the subject for the email. The default is **Offense ID**.
Email Message	Type the standard message that you want to accompany the notification email.

5. Click **Send**.

Marking an offense for follow-up

Mark an offense for follow-up when you want to flag it for further investigation.

Procedure

1. Click the **Offenses** tab.
2. Find the offense that you want to mark for follow-up.
3. Double-click the offense.
4. From the **Actions** list, select **Follow up**.

Results

The offense now displays the follow-up icon in the **Flag** column. To sort the offense list to show flagged offenses at the top, click the **Flags** column header.

Chapter 5. QRadar Analyst Workflow

IBM Security QRadar Analyst Workflow provides new methods for filtering offenses and events, and graphical representations of offenses, by magnitude, assignee, and type. The improved offenses workflow provides a more intuitive method to investigate offense to determine the root cause of an issue and work to resolve it. Use the built-in query builder to create AQL queries by using examples and saved or shared searches, or by typing plain text into the search field.

Offenses
: The Offenses page displays a table of the offenses in your QRadar environment that you can filter in many different ways. It also includes graphical representations of offenses, by magnitude, assignee, and type. From this page, you can investigate an offense to determine the root cause of an issue and work to resolve it.

Search
: The Search page includes a Query Builder that you can use to build an Ariel Query Language (AQL) search to find specific offenses. Create a search using examples, saved or shared searches, or typing directly into the Query Builder. The Search page also includes links to many resources to learn about creating AQL queries.

Apps
: The Apps list includes QRadar apps that are compatible with the new Analyst Workflow. The first release of the workflow includes the Dashboards (Pulse) app. IBM QRadar Pulse is a dashboard app that you can use to communicate insights and analysis about your network. For more information, see the IBM QRadar Pulse documentation.

See the QRadar Analyst Workflow announcement on the IBM Security Community Announcement Blog.

What's new in QRadar Analyst Workflow

Learn about new features and capabilities that make it easier for you to monitor offenses in QRadar Analyst Workflow.

Version 2.15.10

For new features and fixed issues, see the QRadar Analyst Workflow 2.15.10 release notes: https://www.ibm.com/support/pages/node/6563861.

IBM Security QRadar Analyst Workflow Known Issues

QRadar Analyst Workflow contains required information for known issues.

QRadar Analyst Workflow 2.15.10

If you view event data by using the custom rules redirect, the query does not display. To work around this problem, refresh the page to view the data.

Installing the stand-alone version

You can install IBM Security QRadar Analyst Workflow on QRadar 7.4.0 or later.

About this task

The following instructions describe the installation process for QRadar versions 7.4.0 to 7.4.3 GA only. For installations with QRadar version 7.4.3 Fix Pack 1 and later, IBM Security QRadar Analyst Workflow is installed as a standard application by using extensions management. For more information, see "Installing the UBI app version" on page 47.

© Copyright IBM Corp. 2012, 2021

The stand-alone version of QRadar Analyst Workflow requires root access to install. If you are using the command line to enable root user privileges, you must use the following command:

```
sudo su -
```

If you use sudo su (without -), full root access is not granted.

Procedure

1. If you have custom certificates, run the following commands on your QRadar Console, in any directory:
   - update-ca-trust
   - systemctl restart docker
2. Download the latest version of the QRadarAnalystWorkflow<*x.x.x*>.zip file from Fix Central. See instructions on the IBM Security App Exchange.
3. Copy the file onto your QRadar host by using the Linux "secure copy" (scp) command or an FTP client.

   Secure copy example: scp QRadarAnalystWorkflow<*x.x.x*>.zip <*QRadar host*>:/ <*directory*>
4. Type the following command to create a new directory on the QRadar host: mkdir qradar-ui

   Note: If the directory exists from a previous installation, you must delete it before you extract the .zip file.
5. To extract the latest version of the QRadarAnalystWorkflow<*x.x.x*>.zip file on your QRadar host, type the following command: rm -rf qradar-ui && unzip QRadarAnalystWorkflow<*x.x.x*>.zip -d qradar-ui
6. Run ./qradar-ui/start.sh, then wait for the logs to run.
7. Access the QRadar Analyst Workflow by using one of the following methods:
   - In the navigation menu, click **Try the New UI**.
   - Access the new UI in your browser at https://<*QRadar IP address*>/console/ui.

   Tip: For more information, see this helpful video about installing the QRadar Analyst Workflow.

Removing the stand-alone version

If you upgrade to QRadar version 7.4.3 Fix Pack 1 or later, you must uninstall the IBM Security QRadar Analyst Workflow stand-alone version.

Procedure

1. To stop the QRadar Analyst Workflow, run the following commands in order.

```
/opt/ibm/si/conman/bin/conman-api-cli.sh stop -n ui -f

/opt/ibm/si/conman/bin/conman-api-cli.sh stop -n graphql -f
```

2. To remove the Docker images, run the following command.

```
docker images
```

3. Obtain the container ID and graphical ID from your system administrator, and run the followingcommand.

```
docker image rm <ui-container-id> <graphql-container-id>
```

4. To remove the folder extracted from Step 3, for example rm -rf qradar-ui, run the following commands in order.

```
cd /root
```

```
rm -rf qradar-ui
```

5. To remove the application, run the following commands in order.

```
/opt/ibm/si/conman/bin/conman-api-cli.sh remove -n ui -f

/opt/ibm/si/conman/bin/conman-api-cli.sh remove -n graphql -f
```

What to do next

After you uninstall the stand-alone version, you can Install the UBI app version.

Installing the UBI app version

After you download the Red Hat Universal Base Images (UBI) app version of the IBM Security QRadar Analyst Workflow from the IBM Security App Exchange, install it by using the **Extensions Management** page on your QRadar computer.

Before you begin

You must have an IBM ID to access the App Exchange.

Important: The UBI version is supported on QRadar 7.4.3 Fix Pack 1 or later.

About this task

For more information about UBI, see QRadar: Applications, CentOS 6, and Python 2 End of Support (https://www.ibm.com/support/pages/node/6356547).

Important: If you upgrade to QRadar version 7.4.3 Fix Pack 1 or later, you must uninstall the QRadar Analyst Workflow stand-alone version before you install the UBI app version. For instructions, see "Removing the stand-alone version" on page 46.

Procedure

1. Download the QRadar Analyst Workflow UBI app archive from the IBM Security App Exchange (https:// exchange.xforce.ibmcloud.com/hub/extension/ec3471adfdbb0b7bb3fbcf60f0ba5837) onto your local computer.
2. On the QRadar Console, click **Admin** > **Extensions Management**.
3. In the **Extension Management** window, click **Add** and select the app archive that you want to upload to the console.
4. Select the **Install immediately** checkbox.

   Important: You might have to wait several minutes before your app becomes active.
5. To preview the contents of an app after it is added and before it is installed, select it from the list ofextensions, and click **More Details**. Expand the folders to view the individual content items in each group.
6. Access the QRadar Analyst Workflow by using one of the following methods:

- In the navigation menu, click **Try the New UI**.
- Access the new UI in your browser at https://<*QRadar IP address*>/console/ui.

What to do next

When the installation is complete, clear your browser cache and refresh the browser window before you use the app.

Offenses

The QRadar Analyst Workflow Offenses overview page displays a table of the offenses in your QRadar environment that you can filter in many different ways. It also includes graphical representations of offenses, by magnitude, assignee, and type.

On the offenses page, you can investigate an offense to determine the root cause of an issue and work to resolve it.

Tip: For more information about investigating offenses in QRadar Analyst Workflow, see this video walkthrough about offenses.

Visualization of offenses

Filter the Offenses table in the QRadar Analyst Workflow to display the specific offenses you want to investigate.

About this task

As you apply filters, the offenses table displays only the offenses that meet your filter criteria. The graphs displayed on the page also change to reflect only the offenses in your filtered list.

Tip: You can copy and paste the URL from your browser to share the offenses page, including all filters and configuration options.

Procedure

1. To apply a filter, click any of the following categories to see filtering options for that category:
   - Magnitude
   - Severity
   - Assigned To
   - Status
   - Start Time
   - Offense Type
   - Log Source Name
   - Log Source Type
   - Destination Network
   - Local Destination Addresses
   - Source Addresses
   - Rules
   - Follow Up
   - Protected
2. To include only offenses with specific attributes, select that attribute in the filters list. To exclude offenses with specific attributes, click the icon next to the attribute, and click **Apply IS NOT Filter**.

Tip: You can right-click on a Status, Type, Source IP, or Destination IP in the offenses table and quickly apply an IS or IS NOT filter to the offenses.

3. To sort the offenses table in ascending or descending order by an attribute, click the appropriate tableheading.
4. To clear individual filters, click the **X** on the filter indicator. To clear all filters, click **Clear filters**.
5. To configure the number of offenses displayed in the table, click the **Items per page** drop-down at the bottom of the table.
6. To sort the offenses table in ascending or descending order by an attribute, click the appropriate tableheading.

Offense investigation

Begin your offense investigation in the QRadar Analyst Workflow by clicking an offense in the offense table. The offense details provide context to help you understand what happened and determine how to isolate and resolve the problem.

In addition to the basic information included in the offense table, the offense details page includes the following detailed information:

Feature	**Description**
Insights	The Insights section displays rules that triggered the event. Click a rule to see details about specific rules.
Events graph	The Events graph displays the number of events that occurred at a given time within the last 7 active days. Use the scrubber bar at the top of the graph to zoom in on specific times and event spikes. Click **View Events** to see a list of events that contributed to the offense and investigate event details.
Source and Destination IPs	If offenses include multiple source or destination IPs, you can click the IP lists to scroll through the entire list of IPs. Click a specific IP address to see details about that IP.
Magnitude	The Magnitude graph provides a visual representation of how the magnitude was calculated, based on relevance, credibility, and severity. Click the graph to see a detailed description of how the magnitude is calculated.
Notes	In the Notes section, you can click on a long note to see the entire text. Click **Add note** to add your own note to the offense details.

Tip: If an offense has a long title, click on the title to see the entire offense title.

Offense actions

Use the QRadar Analyst Workflow to keep track of offenses throughout your investigation.

Knowing that an offense occurred is only the first step; identifying how it happened, where it happened, and who did it requires some investigation.

Marking an offense for follow-up

In the QRadar Analyst Workflow, you can mark an offense for follow-up when you want to flag it for further investigation.

Procedure

1. From the Offenses table, do one of the following actions:
   - Select the offenses that you want to flag.
   - Click on a single offense listing to open the offense details.
2. From the **Actions** list, select **Follow up**.

   Tip: To remove the flag, select **Unfollow** from the **Actions** list.

Protecting offenses

You might have offenses that you want to retain regardless of the retention period. In the QRadar Analyst Workflow, you can protect offenses to prevent them from being removed from QRadar after the retention period has elapsed.

About this task

By default, offenses are retained for thirty days. For more information about customizing the offense retention period, see the *IBM QRadar Administration Guide*.

Procedure

1. From the Offenses table, do one of the following:
   - Select any offenses you want to protect.
   - Click on a single offense listing to open the offense details.
2. From the **Actions** list, select **Protect**.

   Tip: To remove the protection from the offense, select **Unprotect** from the **Actions** list.

Hiding offenses

Hide an offense to prevent it from being displayed in the QRadar Analyst Workflow offenses table. After you hide an offense, the offense is only displayed if you apply an IS filter for **Status = Hidden**.

Procedure

1. From the Offenses table, do one of the following:
   - Select any offenses you want to hide.
   - Click on a single offense listing to open the offense details.
2. From the **Actions** list, select **Hide**.

   Tip: To unhide the offense, filter to see hidden offenses, and select **Open** from the **Actions** list.

Closing offenses

Close an offense in the QRadar Analyst Workflow to remove it completely from your system.

About this task

The default offense retention period is 30 days. After the offense retention period expires, closed offenses are deleted from the system. You can protect an offense to prevent it from being deleted when the retention period expires.

After you close an offense, the offense is only displayed if you apply an IS filter for **Status = Closed**. If more events occur for an offense that is closed, a new offense is created.

When you close offenses, you must select a reason for closing the offense. If you have the **Manage Offense Closing** permission, you can add custom closing reasons. For more information about user role permissions, see the *IBM QRadar Administration Guide*.

Procedure

1. From the Offenses table, do one of the following:
   - Select any offenses you want to close.
   - Click on a single offense listing to open the offense details.
2. From the **Actions** list, select **Close**.
3. Specify a closing reason from the **Choose a resolution option** list.
4. In the text field, type a note to provide more information.

   Notes must not exceed 1,984 characters.
5. Click **OK**.

Querying event and flow data to find specific offenses

Search for specific event and flow data by creating Ariel Query Language (AQL) searches in the QRadar Analyst Workflow Query Builder.

About this task

Create searches by using search history or entering keywords directly into the Query Builder. This information populates a query template that you can further customize to suit your needs, or manually create your own searches.

Tip: To build a query without using AQL, try the Visual query builder.

Procedure

1. From the navigation menu (☰), click **Search**, and select the **Advanced builder** tab.
2. Type one of the following keywords in the **Query Builder** to start a query:
   - IP address
   - URL
   - MD5/SHA-1/SHA-256 hash
3. Select one of the predefined searches from the list that appears as you enter a keyword.
4. Review and edit the query template to refine your search, and then click **Run query**.

   Tip:
   - Syntax tokens are color-coded based on token class.

- For a syntactically correct AQL string, paired parentheses are underscored when the cursor is placedbetween them.

```
(startTime, 'MMM dd hh:mm a')
```

5. Click **Filter** to further refine your search results and then select an offense to view more details.
6. To run an existing search result, select the query in the **Last Search** field to add it to the Query Builder, and then click **Run query**.
7. Optional: Expand the **Training and resources** section to learn more about AQL queries.

Example

The following is an example of an AQL query.

```
SELECT sourceip, destinationip, username
FROM events
WHERE username = 'test name'
GROUP by sourceip, destinationip
ORDER BY sourceip DESC
LIMIT 10
LAST 2 DAYS
```

For more information about creating queries in QRadar Analyst Workflow, see this video walkthrough about the Search feature (https://youtu.be/GjITI5aFvPU).

For more information about AQL queries, see these documentation and training resources:

- Introduction to AQL with sample queries (https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/r_qradar_aql_intro_AQL_queries.html)
- Overview of Ariel Query Language (https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_aql_introduction.html)
- AQL logical and comparison operators (https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/r_aql_operators.html)
- QRadar AQL tutorial part 1: Documentation and basic syntax (https://youtu.be/-ZHVubxGO2s)
- QRadar AQL tutorial part 2: Very useful AQL functions (https://youtu.be/KfXrij5hGSM)

Related concepts Offense investigation

Begin your offense investigation in the QRadar Analyst Workflow by clicking an offense in the offense table. The offense details provide context to help you understand what happened and determine how to isolate and resolve the problem.

Related tasks

Visualization of offenses

Filter the Offenses table in the QRadar Analyst Workflow to display the specific offenses you want to investigate.

Searching with the visual query builder

You can use the visual builder to search for specific event and flow data without any knowledge of Ariel Query Language (AQL).

Procedure

1. From the navigation menu (☰), click **Search**, and select the **Visual builder** tab.
2. If you want to enable quick filtering of simple terms from your results, toggle the **Quick Filter** switch, type a value to filter, and press Enter.
3. Select a boolean **IF** operator for your condition set.
   - **AND** includes only data that meets all of the conditions in your set.
   - **OR** includes data that meets any of the conditions in your set.
4. Select a **Condition** to search for.

   Examples include source or destination IP addresses, geographic locations, event names, log sources, and many more.
5. Select an Operator, such as **Equals**, **Does not equal**, or a value specific to that condition.
6. Type or select a **Value**, or use the toggle icon to display child values.
7. To add more conditions to your set, click **Add another condition**, then repeat Steps 4 - 6 to define each condition.
8. To add another condition set to your query, click **Add condition set**, select the **AND** or **OR** boolean operator, then repeat Steps 4 - 6 to define each condition in the new set.
9. After you finish defining conditions, click **Run Search**.

Events

Use the QRadar Analyst Workflow Events page to further investigate specific events to determine the root cause of an issue and work to resolve it.

The Events page displays a table of the events that contributed to a specific offense and a Time Series chart that shows the number of events sorted by date. You can filter these events to suit your needs.

Related concepts Offense investigation
Begin your offense investigation in the QRadar Analyst Workflow by clicking an offense in the offense table. The offense details provide context to help you understand what happened and determine how to isolate and resolve the problem.

Offense actions
Use the QRadar Analyst Workflow to keep track of offenses throughout your investigation.

Investigating events

The Events graph on the QRadar Analyst Workflow offense details page displays the number of events that occurred at a given time within the last 7 active days.

Procedure

1. From the offenses page, click on an offense in the offense table to open the details page.

   Tip: Use the scrubber bar at the top of the Events graph to zoom in on specific times and event spikes.
2. Click **View Events** to see a list of events that contributed to the offense and investigate event details.
3. To configure the number of events returned in your filter results, click the arrows in the Result Limit indicator.
4. To configure the number of events displayed in the table, click the Items per page drop-down at the bottom of the table.

5. To sort the events table in ascending or descending order by an attribute, click the appropriate tableheading.
6. Click on an event to see more details about that event. You can also click on a log source, source IP, ordestination IP for specific information on that source or destination.
7. Click **Update events** to refresh the events results.

   Tip: You can copy and paste the URL from your browser to share the events page, including all filters and configuration options.

Filtering events

Filter the QRadar Analyst Workflow Events page to display only the specific events you want to investigate.

About this task

As you apply filters, the events table displays only the events that meet your filter criteria.

Tip: You can copy and paste the URL from your browser to share the events page, including all filters and configuration options.

Procedure

1. To apply a filter, click any of the following categories to see filtering options for that category:
   - Event Time
   - Magnitude
   - Log Source Name
   - Category
   - Source IP
   - Source Port
   - Destination IP
   - Destination Port
   - Event Name
   - User
2. To include only events with specific attributes, select that attribute in the filters list. To exclude events with specific attributes, click the vertical ellipsis icon [⋮] next to the attribute, and click **Apply IS NOT Filter**.

   Tip: You can right-click on a Log Source, Source IP, Destination IP, Category, or Username in the events table and quickly apply an IS or IS NOT filter to the events.
3. To sort the events table in ascending or descending order by an attribute, click the appropriate tableheading.
4. To clear individual filters, click the close icon [x] on the filter indicator. To clear all filters, click **Clear filters**.
5. Click **Update events** to refresh the events results.

Chapter 6. Log activity investigation

You can monitor and investigate 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.

Tip: You can also investigate log activity using the IBM QRadar Analyst Workflow interface. For more information, see Chapter 5, "QRadar Analyst Workflow," on page 45.

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.

The **Log Activity** tab specifies which events are associated with offenses.

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 8. Log Activity toolbar options

Option	Description
Search	Click **Search** to perform advanced searches on events. Options include: • **New Search** - Select this option to create a new event search. • **Edit Search** - Select this option to select and edit an event search. • **Manage Search Results** - Select this option to view and manage search results.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the **Quick Searches** list box only when you have saved search criteria that specifies the **Include in my Quick Searches** option.
Add Filter	Click **Add Filter** to add a filter to the current search results.
Save Criteria	Click **Save Criteria** to save the current search criteria.

Save Results	Click **Save Results** to save the current search results. This option is only displayed after a search is complete. This option is disabled in streaming mode.
Cancel	Click **Cancel** to cancel a search in progress. This option is disabled in streaming mode.

© Copyright IBM Corp. 2012, 2021

Table 8. Log Activity toolbar options (continued)

Option	**Description**
False Positive	Click **False Positive** to open the **False Positive Tuning** window, which will allow you to tune out events that are known to be false positives from creating offenses. This option is disabled in streaming mode. For more information about tuning false positives, see Tuning false positives.
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 8. Log Activity toolbar options (continued)

Option	Description

Rules (continued)	• **Add Behavioral Rule** - 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. When you select the **Add Behavioral Rule** option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a behavioral rule. • **Add Anomaly Rule** - 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. When you select the **Add Anomaly Rule** option, the Rules wizard is displayed, prepopulated with the appropriate options for creating an anomaly rule.

Table 8. Log Activity toolbar options (continued)

Option	**Description**

Actions	Click **Actions** to perform the following actions: • **Show All** - Select this option to remove all filters on search criteria and display all unfiltered events. • **Print** - Select this option to print the events that are displayed on the page. • **Export to XML** > **Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events. • **Export to XML** > **Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events. • **Export to CSV** >**Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See Exporting events. • **Export to CSV** > **Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See Exporting events. • **Delete** - Select this option to delete a search result. See Managing event and flow search results. • **Notify** - Select this option to specify that you want a notification emailed to you on completion of the selected searches. This option is only enabled for searches in progress. **Note:** The **Print**, **Export to XML**, and **Export to CSV** options are disabled in streaming mode and when viewing partial search results.
Search toolbar	**Advanced Search** Select **Advanced Search** from the list box to enter an Ariel Query Language (AQL) search string to specify the fields that you want returned. **Quick Filter** Select Quick Filter from the list box to search payloads by using simple words or phrases.
View	The default view on the **Log Activity** tab is a stream of real-time events. The **View** list contains options to also view events from specified time periods. After you choose a specified time period from the **View** list, you can then modify the displayed time period by changing the date and time values in the **Start Time** and **End Time** fields.

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 9. Right-click menu options

Option	**Description**
Filter on	Select this option to filter on the selected event, depending on the selected parameter in the event.
False Positive	Select this option to open the **False Positive** window, which will allow you to tune out events that are known to be false positives from creating offenses. This option is disabled in streaming mode. See Tuning false positives.
More options:	Select this option to investigate an IP address or a user name. For more information about investigating an IP address, see Investigating IP addresses. **Note:** This option is not displayed in streaming mode.
Quick Filter	Filter items that match, or do not match the selection.

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, allowing you to view events in real time.

For more information about streaming mode, see Viewing streaming events. You can specify a different time range to filter events 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.

By default, the **Log Activity** tab displays the following parameters when you view normalized events:

Table 10. Log Activity tab - Default (Normalized) parameters

Parameter	Description
Current® Filters	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.
View	From this list box, you can select the time range that you want to filter for.

Table 10. Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description

Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: **Note:** Click the arrow next to **Current Statistics** to display or hide the statistics • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. **Note:** Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.
Charts	Displays configurable charts 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. For more information about configuring charts, see Chart management. **Note:** If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To displayed charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.
Offenses icon	Click this icon to view details of the offense that is associated with this event. For more information, see Chart management. **Note:** Depending on your product, this icon is might not be available. You must have IBM QRadar SIEM.
Start Time	Specifies the time of the first event, as reported to QRadar by the log source.
Event Name	Specifies the normalized name of the event.

Table 10. Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description
Log Source	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.
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 detected within a short time.
Time	Specifies the date and time when QRadar received the event.
Low Level Category	Specifies the low-level category that is associated with this event. For more information about event categories, see the *IBM QRadar Administration Guide*.
Source IP	Specifies the source IP address of the event. **Note:** If you select the **Normalized (With IPv6 Columns)** display, refer to the **Source IPv6** parameter for IPv6 events.
Source Port	Specifies the source port of the event.
Destination IP	Specifies the destination IP address of the event. **Note:** If you select the **Normalized (With IPv6 Columns)** display, refer to the **Destination IPv6** parameter for IPv6 events.
Destination Port	Specifies the destination port of the event.
Username	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.
Magnitude	Specifies the magnitude of this event. Variables include credibility, relevance, and severity. Point your mouse over the magnitude bar to display values and the calculated magnitude.

If you select the **Normalized (With IPv6 Columns)** display, then the **Log Activity** tab displays the following extra parameters:

Table 11. Log Activity tab - Normalized (With IPv6 Columns) parameters

Parameter	Description

Source IPv6	Specifies the source IP address of the event. **Note:** IPv4 events display 0.0.0.0.0.0.0.0 in the **Source IPv6** and **Destination IPv6** columns.

Table 11. Log Activity tab - Normalized (With IPv6 Columns) parameters (continued)

Parameter	Description
Destination IPv6	Specifies the destination IP address of the event. **Note:** IPv4 events display 0.0.0.0.0.0.0.0 in the **Source IPv6** and **Destination IPv6** columns.

Procedure

1. Click the **Log Activity** tab.
2. Optional: From the **Display** list box, select **Normalized (With IPv6 Columns)**.
   The **Normalized (With IPv6 Columns)** display shows source and destination IPv6 addresses for IPv6 events.
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

Parameter	Description
Current Filters	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.
View	From this list box, you can select the time range that you want to filter for.

Table 12. Raw Event parameters (continued)

Parameter	Description

Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: **Note:** Click the arrow next to **Current Statistics** to display or hide the statistics • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. **Note:** Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.
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 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.
Offenses icon	Click this icon to view details of the offense that is associated with this event.
Start Time	Specifies the time of the first event, as reported to QRadar by the log source.
Log Source	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.
Payload	Specifies the original event payload information in UTF-8 format.

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

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

Table 13. Grouped events options (continued)	
Group option	**Description**
Source Port	Displays a summarized list of events that are grouped by the source port address of the event.

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

Table 14. Grouped event parameters	
Parameter	**Description**
Grouping By	Specifies the parameter that the search is grouped on.
Current Filters	The top of the table displays the details of the filter that is applied to the search results. To clear these filter values, click **Clear Filter**.
View	From the list box, select the time range that you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: **Note:** Click the arrow next to **Current Statistics** to display or hide the statistics. • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. **Note:** Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.

Table 14. Grouped event parameters (continued)	
Parameter	**Description**

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 toview more information about the parameters it represents. • Right-click the legend item to further investigatethe 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.
Log Source (Unique Count)	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.

Table 14. Grouped event parameters (continued)	
Parameter	**Description**
High Level Category (Unique Count)	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 QRadar Log Manager Administration Guide*.
Low Level Category (Unique Count)	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.
Protocol (Unique Count)	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.
Username (Unique Count)	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.
Magnitude (Maximum)	Specifies the maximum calculated magnitude for grouped events. Variables that are used to calculate magnitude include credibility, relevance, and severity.
Event Count (Sum)	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.
Count	Specifies the total number of normalized events in this event group.

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 moreinformation about event details, see Table 2.

Viewing 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

Parameter	**Description**
Event Name	Specifies the normalized name of the event.
Low Level Category	Specifies the low-level category of this event. For more information about categories, see the *IBM QRadar Administration Guide*.
Event Description	Specifies a description of the event, if available.
Magnitude	Specifies the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.
Relevance	Specifies the relative impact of an event, category, or offense on the network.
Severity	Specifies the relative threat that a source poses on a destination.
Credibility	Specifies the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.
Username	Specifies the user name that is associated with this event, if available. To access more information that is associated with a selected user name, right-click the user name for **View Assets** and **View Events** menu options.
Start Time	Specifies the time of the event was received from the log source.
Storage Time	Specifies the time that the event was stored in the QRadar database.
Log Source Time	Specifies the system time as reported by the log source in the event payload.
Anomaly Detection Information - This pane is only displayed if this event was generated by an anomaly detection rule. Click the **Anomaly** icon to view the saved search results that caused the anomaly detection rule to generate this event.	
Rule Description	Specifies the anomaly detection rule that generated this event.

Anomaly Description	Specifies a description of the anomalous behavior that was detected by the anomaly detection rule.
Anomaly Alert Value	Specifies the anomaly alert value.
Source and Destination information	
Source IP	Specifies the source IP address of the event.

Table 15. Event details (continued)

Parameter	**Description**
Destination IP	Specifies the destination IP address of the event.
Source Asset Name	Specifies the user-defined asset name of the event source. For more information about assets, see Asset management.
Destination Asset Name	Specifies the user-defined asset name of the event destination. For more information about assets, see Asset management
Source Port	Specifies the source port of this event.
Destination Port	Specifies the destination port of this event.
Pre NAT Source IP	For a firewall or another device capable of Network Address Translation (NAT), this parameter specifies the source IP address before the NAT values were applied. NAT translates an IP address in one network to a different IP address in another network.
Pre NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address before the NAT values were applied.
Pre NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port before the NAT values were applied.
Pre NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port before the NAT values were applied.
Post NAT Source IP	For a firewall or another device capable of NAT, this parameter specifies the source IP address after the NAT values were applied.
Post NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address after the NAT values were applied.

Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
Source IPv6	Specifies the source IPv6 address of the event.

Table 15. Event details (continued)

Parameter	**Description**
Destination IPv6	Specifies the destination IPv6 address of the event.
Source MAC	Specifies the source MAC address of the event.
Destination MAC	Specifies the destination MAC address of the event.
Payload information	
Payload	Specifies the payload content from the event. This field offers 3 tabs to view the payload: • Universal Transformation Format (UTF) - ClickUTF. • 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.
Event Collector	Specifies the ID of the Event Collector component that parsed the event.
QID Event ID	The primary value set by a DSM to identify an event. QRadar uses this field together with the Event Category to map to a QID record for the event.
QID Event Category	The secondary value set by a DSM to identify an event. QRadar uses this field together with the Event ID to map to a QID record for the event.

Table 15. Event details (continued)

Parameter	**Description**
Log Source Identifier	Specifies the Log Source Identifier of the log source that received the event. If the event is routed to a **SIM Generic Log** type log source, set this value as the Log Source Identifier value when you create a log source to collect this event.
Truncated	Specifies whether the event payload was truncated because it exceeded the maximum allowable size of 32 KB for QRadar. The parameter is only set to True if the payload was truncated before storage because it exceeded the maximum allowable size for QRadar. The parameter is set to False if the payload was not truncated at all. It is also set to False if the payload was truncated by the log source protocol that collected it based on the maximum payload size parameter that was set in the log source configuration.

Stored for Performance	Set to True if an event was routed directly to storage due to performance problems. If the parameter is set to False, and the event has a Low Level Category of Stored, QRadar attempted to parse it but the event was unrecognized by all available log sources that have a matching Log Source Identifier. In both cases, the event was stored without any parsing or normalization.
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 least one of the following items: User name or MAC address. Not all log sources generate identity information.	
Identity Username	Specifies the user name of the asset 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.
Identity Extended field	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.

Table 15. Event details (continued)

Parameter	**Description**
Has Identity (Flag)	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 QRadar DSM Configuration Guide*.
Identity Host Name	Specifies the host name of the asset that is associated with this event.
Identity MAC	Specifies the MAC address of the asset that is associated with this event.
Identity Group Name	Specifies the group name of the asset that is associated with this event.

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	
Parameter	**Description**
Return to Events List	Click **Return** to **Events List** to return to the list of events.
Offense	Click **Offense** to display the offenses that are associated with the event.
Anomaly	Click **Anomaly** to display the saved search results that caused the anomaly detection rule to generate this event. **Note:** This icon is only displayed if this event was generated by an anomaly detection rule.
Map Event	Click **Map Event** to edit the event mapping. For more information, see Modifying event mapping.
False Positive	Click **False Positive** to tune QRadar to prevent false positive events from generating into offenses.
Extract Property	Click **Extract Property** to create a custom event property from the selected event.
Previous	Click **Previous** to view the previous event in the event list.
Next	Click **Next** to view the next event in the event list.
Table 16. Event details toolbar (continued)	
Parameter	**Description**
PCAP Data	**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. • **View PCAP Information** - Select this option to view the PCAP information. For more information, see Viewing PCAP information. • **Download PCAP File** - Select this option to download the PCAP file to your desktop system. For more information, see Downloading the PCAP file to your desktop system.
Print	Click **Print** to print the event details.

Viewing associated offenses

From the Log Activity tab, you can view the offense that is associated with the event.

About this task

If an event matches a rule, an offense can be generated on the **Offenses** tab.

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

When you view an offense from the **Log Activity** tab, the offense might not display if the Magistrate has not yet saved the offense that is associated with the selected event to disk or the offense has been purged from the database. If this occurs, the system notifies you.

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. Click the **Offense** icon beside the event you want to investigate.
4. View the associated offense.

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 QRadar 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**.

Tuning false positive events from creating offenses

You can use the False Positive Tuning function to prevent false positive events from creating offenses.

Before you begin

You can tune false positive events from the **event list** or **event details** page.

About this task

You can tune false positive events from the **event list** or **event details** page.

You must have appropriate permissions for creating customized rules to tune false positives.

For more information about roles, see the *IBM QRadar Administration Guide*.

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. Select the event that you want to tune.
4. Click **False Positive**.
5. In the Event/Flow Property pane on the **False Positive** window, select one of the following options:
   - Event/Flow(s) with a specific QID of <Event>
   - Any Event/Flow(s) with a low-level category of <Event>
   - Any Event/Flow(s) with a high-level category of <Event>
6. In the Traffic Direction pane, select one of the following options:
   - <Source IP Address> to <Destination IP Address>
   - <Source IP Address> to Any Destination
   - Any Source to <Destination IP Address>
   - Any Source to any Destination
7. Click **Tune**.

Related tasks Tuning false positives

You can prevent false positive flows from creating offenses. You can tune false positive flows from the flow list or flow details page.

PCAP data

If your QRadar Console is configured to integrate with the Juniper JunOS Platform DSM, then Packet Capture (PCAP) can be received, processed, 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 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 7. Network activity monitoring

IBM QRadar collects information about the way that devices in your network communicate with each other. The record of the communication as it occurs across the network is called a *flow*.

In QRadar, flows appear on the **Network activity** tab, and you must have permissions to view it.

By default, the **Network Activity** tab displays flows in streaming mode. To analyze flows that were already received, you can pause streaming mode, and conduct searches and apply filters to the flows.

If you previously configured a saved search as the default, the results of that search are automatically displayed when you access the **Network Activity** tab.

Difference between events and flows

An *event* is a record of an activity that occurred on your network at a single point in time. It provides information about an activity that happened and which assets were implicated. For example, if a user tries to authenticate against your firewall and is unsuccessful, the firewall sends a system log to QRadar. The authentication attempt is recorded as an event. You view information about events on the **Log Activity** tab.

Unlike an event, a flow is network activity that occurs over time. The flow record shows the actual messages that were sent and received by devices as they communicated with each other over the network. For example, a flow might show when a user sends an email, goes to a web page, downloads a file, or uses social media. The web request might download files such as images and ads over a few seconds, or last a few hours if the user is watching a movie.

Compared to events, flow traffic provides a complete view of what is happening on your network. They show you what was happening before, during, and after the event occurred.

Flow pipeline

Flows that come into IBM QRadar go through an in-depth process to extract additional information about the network communication, looking for indicators that a security incident might have occurred.

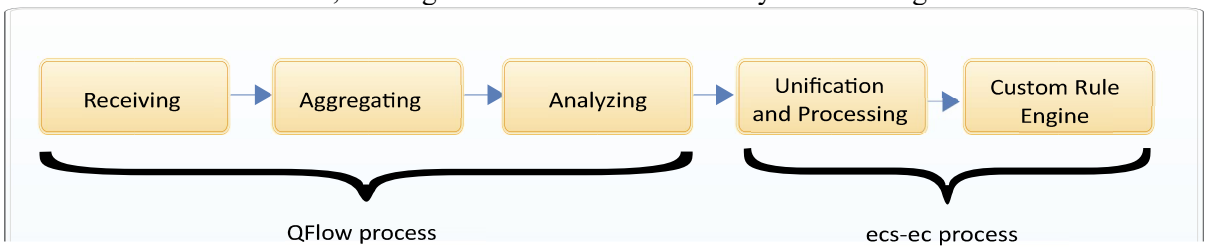


Figure 4. Flow pipeline in QRadar

QFlow process

The QFlow process collects data from a variety of flow sources. It aggregates the data by parsing and normalizing the data, accruing information over a one minute period. It then analyzes the flow to extract additional information such as determining the application and flow direction, and creating superflows before handing it off to the ecs-ec process.

ecs-ec process

The ecs-ec process further parses the flow record and performs additional unification and processing, such as deduplication, asymmetric recombination, licensing, domain tagging, custom flow properties, and flow forwarding. The flow is then passed to the Custom Rule Engine (CRE) to determine if the flow triggers a rule, which might indicate that a security incident has occurred.

© Copyright IBM Corp. 2012, 2021

Flow sources

IBM QRadar can receive flows from many different types of flow sources. The flow sources are classified as either internal or external.

Internal flow sources

Internal flow sources collect raw packets from either a network tap device or a span or mirror port that is connected to a Napatech or network interface card. These sources provide raw packet data as it appears on the network, and sends it to a monitoring port on a QRadar Flow Collector, which converts the packet data into flow records.

Internal flow sources can be multithreaded. QRadar does not keep the entire packet payload. Instead, it captures only some of the packets from the beginning of the communication. This snapshot is referred to as the *payload* or *content capture*.

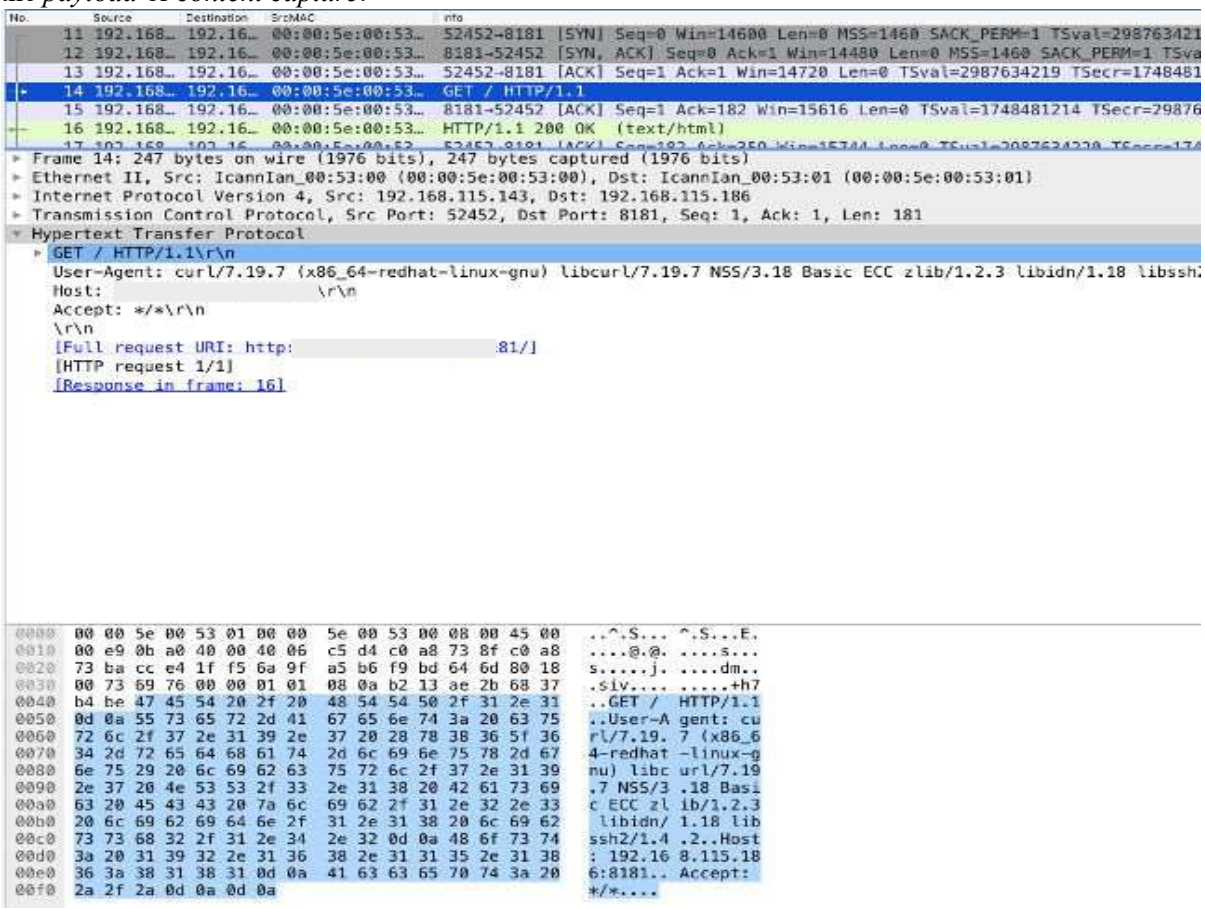


Figure 5. Packet capture from an internal flow source

External flow sources

QRadar also supports external flow sources, such as routers that send common network monitoring protocols, such as NetFlow, IPFIX, sFlow J-Flow, and Packeteer data.

These external flow sources can provide a different level of visibility than internal flow sources. For example, NetFlow records can provide both the router interface that the packets crossed, as well as the ASN record numbers of the originating network. When using IPFIX, additional fields that are not parsed into normalized fields can be placed into the payload as name value pairs, which can then be used as custom properties.

External sources do not require as much CPU utilization to process so you can send them directly to a Flow Processor. In this configuration, you can have a dedicated flow collector and a flow processor, both receiving and creating flow data.

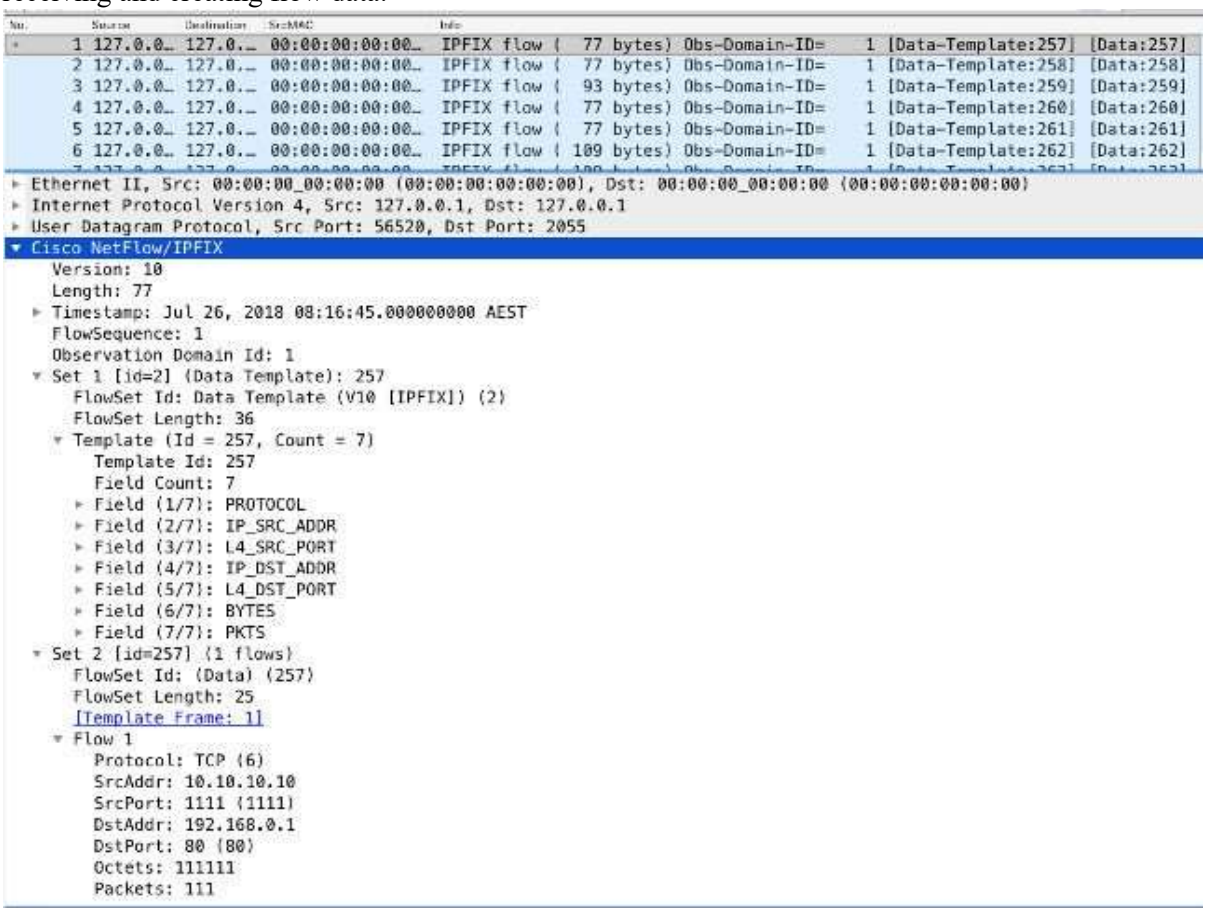


Figure 6. Packet capture from an external flow source

NetFlow

NetFlow is a proprietary accounting technology that is developed by Cisco Systems. NetFlow monitors traffic flows through a switch or router, and interprets the client, server, protocol, and port that is used. It also counts the number of bytes and packets, and sends that data to a NetFlow collector.

The process of sending data from NetFlow is often referred to as a NetFlow Data Export (NDE).

IBM QRadar accepts NetFlow Data Exports (NDE) so that it functions as a NetFlow collector. QRadar supports NetFlow versions 1, 5, 7, and 9.

While NetFlow expands the amount of the network that is monitored, it uses a connection-less protocol (UDP) to deliver NDEs. After an NDE is sent from a switch or router, the NetFlow record is purged. UDP doesn't guarantee the delivery of data. As a result, inaccurate presentations of both traffic volumes and bidirectional flows, and reduced alerting capabilities, might result with a NetFlow flow source.

For more information about NetFlow, see the Cisco web site (http://www.cisco.com).

NetFlow flow source configuration

When you configure an external flow source for NetFlow, you must do the following tasks:

- Make sure that the appropriate firewall rules are configured.

If you change your **External Flow Source Monitoring Port** parameter in the Flow Collector configuration, you must also update your firewall access configuration.

- Make sure that the appropriate ports are configured for your Flow Collector.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

NetFlow flow source template

IBM suggests that, at minimum, the following fields are included in the NetFlow flow source template:

- FIRST_SWITCHED
- LAST_SWITCHED• PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

Supported fields

The following lists show some of the types of fields that are supported for NetFlow flow sources.

VLAN fields

The following VLAN fields are supported for NetFlow:

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

MAC address fields

The following MAC address fields are supported for NetFlow:

- sourceMacAddress (56)

- postDestinationMacAddress (57)
- DestinationMacAddress (80)
- postSourceMacAddress (81)

For more information about each field, see the IANA information element assignment at IP Flow Information Export (IPFIX) Entities (https://www.iana.org/assignments/ipfix/ipfix.xhtml).

Related tasks

Configuring a flow collector

Related information

Adding or editing a flow source

IPFIX

Internet Protocol Flow Information Export (IPFIX) is an accounting technology that monitors traffic flows through a switch or router. It interprets the traffic to determine the client, server, protocol, and port that is used. It also counts the number of bytes and packets, and sends that data to an IPFIX collector. IBM Security Network Protection XGS 5000, a next generation intrusion protection system (IPS), is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE), but IPFIX provides more flow information and deeper insight than NetFlow v9.
IBM QRadar accepts NDEs so that it functions as an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After an NDE is sent from the IPFIX forwarding device, the IPFIX record might be purged.

IPFIX flow source configuration

When you configure an external flow source for IPFIX, you must do the following tasks:

- Add a NetFlow flow source.

Note: Your QRadar system might include a default NetFlow flow source. If it does, QRadar can use the default NetFlow flow source to process the IPFIX flows.

To confirm that your system includes a default NetFlow flow source, on the **Admin** tab, select **Flow Sources**. If **default_Netflow** is listed in the flow source list, IPFIX is already configured.

- Ensure that the appropriate firewall rules are configured.

If you change your **External Flow Source Monitoring Port** parameter in the Flow Collector configuration, you must also update your firewall access configuration.

- Ensure that the appropriate ports are configured for your Flow Collector.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

IPFIX flow source template

Ensure that the IPFIX template from the IPFIX source includes the following IANA-listed Information Elements:

- protocolIdentifier (4)
- sourceIPv4Address (8)
- destinationIPv4Address (12)
- sourceTransportPort (7)
- destinationTransportPort (11)

- octetDeltaCount (1) or postOctetDeltaCount (23)• packetDeltaCount (2) or postPacketDeltaCount (24)
- tcpControlBits (6) (TCP flows only).
- flowStartSeconds (150) or flowStartMilliseconds (152) or flowStartDeltaMicroseconds (158)
- flowEndSeconds (151) or flowEndMilliseconds (153) or flowEndDeltaMicroseconds (159)

Supported fields

The following lists show some of the types of fields that are supported for IPFIX flow sources.

New in 7.4.3 To add support for additional IPFIX fields that are not shown by QRadar, you can use the /api/ariel/taggedfields API to create a new tagged field.

VLAN fields

The following VLAN fields are supported for IPFIX:

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

MAC address fields

The following MAC address fields are supported for IPFIX:

- sourceMacAddress (56)
- postDestinationMacAddress (57)
- DestinationMacAddress (80)
- postSourceMacAddress (81)

MPLS fields

The following MPLS fields are supported for IPFIX:

- mplsTopLabelType
- mplsTopLabelIPv4Address
- mplsTopLabelStackSection
- mplsLabelStackSection2
- mplsLabelStackSection3
- mplsLabelStackSection4
- mplsLabelStackSection5
- mplsLabelStackSection6
- mplsLabelStackSection7
- mplsLabelStackSection8

- mplsLabelStackSection9
- mplsLabelStackSection10
- mplsVpnRouteDistinguisher
- mplsTopLabelPrefixLength
- mplsTopLabelIPv6Address
- mplsPayloadLength
- mplsTopLabelTTL
- mplsLabelStackLength
- mplsLabelStackDepth• mplstopLabelExp
- postMplsTopLabelExp
- pseudoWireType
- pseudoWireControlWord
- mplsLabelStackSection
- mplsPayloadPacketSection
- sectionOffset
- sectionExportedOctets

Related tasks
Configuring a flow collector
Related information
Adding or editing a flow source

sFlow

sFlow is a multi-vendor and user standard for sampling technology that provides continuous monitoring of application-level traffic flows on all interfaces simultaneously.

An sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. sFlow traffic is based on sampled data and, therefore, might not represent all network traffic.

IBM QRadar supports flow sources for sFlow versions 2, 4, and 5.

sFlow uses a connection-less protocol (UDP). When data is sent from a switch or router, the sFlow record is purged. UDP doesn't guarantee delivery of the data. As such, inaccurate presentations of both traffic volumes and bidirectional flows, and reduced alerting capabilities, might result when using an sFlow flow source.

For more information, see the sFlow website (www.sflow.org). **sFlow**

flow source configuration

When you configure an external flow source for sFlow, you must do the following tasks:

- Ensure that the appropriate firewall rules are configured.
- Ensure that the appropriate ports are configured for your QRadar VFlow Collector.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

Related tasks
Configuring a flow collector

Related information
Adding or editing a flow source

J-Flow

J-Flow is a proprietary accounting technology used by Juniper Networks that allows you to collect IP traffic flow statistics.

J-Flow enables you to export data to a UDP port on a J-Flow collector. You can also enable J-Flow on a router or network interface to collect network statistics for specific locations on your network.

J-Flow uses a connection-less protocol (UDP). When data is sent from a switch or router, the J-Flow record is purged. UDP doesn't guarantee delivery of the data. As such, inaccurate presentations of both traffic volumes and bidirectional flows, and reduced alerting capabilities, might result when using a J-Flow flow source. J-Flow traffic is based on sampled data and, therefore, might not represent all network traffic.

For more information about J-Flow, see the Juniper Networks website (www.juniper.net).

J-Flow flow source configuration

When you configure an external flow source for J-Flow, you must do the following tasks:

- Ensure that the appropriate firewall rules are configured.
- Ensure that the appropriate ports are configured for your IBM QRadar QFlow Collector.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

Supported VLAN fields

The following VLAN fields are supported for J-Flow:

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- dot1qDEI
- dot1qCustomerDEI
- postDot1qVlanId
- postDotqCustomerVlanId

Related tasks
Configuring a flow collector
Related information
Adding or editing a flow source

Packeteer

Packeteer devices collect, aggregate, and store network performance data.

After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to IBM QRadar.

Packeteer uses a connection-less protocol (UDP). When data is sent from a switch or router, the Packeteer record is purged. Because UDP doesn't guarantee delivery of the data, inaccurate presentations of both traffic volumes and bidirectional flows, and reduced alerting capabilities might result when using a Packeteer flow source.

Packeteer flow source configuration

To configure Packeteer as an external flow source, you must do the following tasks:

- Ensure that the appropriate firewall rules are configured.
- Ensure that you configure Packeteer devices to export flow detail records, and configure the Flow Collector as the destination for the data export.
- Ensure that the appropriate ports are configured for your Flow Collector.
- Ensure that the class IDs from the Packeteer devices can automatically be detected by the FlowCollector.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

Related tasks
Configuring a flow collector
Related information
Adding or editing a flow source

Napatech interface

If you installed a Napatech Network Adapter on your IBM QRadar system, you can monitor the packets that the card sees. The Napatech card must be installed for QRadar to show it in the list of configurable packet-based flow sources.

After the flow source is configured and the changes are deployed, you can view the network traffic on the **Network Activity** tab. You can customize the way that QRadar processes the network traffic by changing the configuration settings, such as the application detection, superflow thresholds, flow direction configuration, and network hierarchy. You can also write rules, perform queries, and filter the network traffic.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

For more information about the Napatech Network Adapter, see the Napatech documentation.

Related tasks
Configuring a flow collector
Related information
Adding or editing a flow source

Network interface

IBM QRadar can monitor packets that come in on any network interface card that is installed on your system. The network interface card must be installed for QRadar to show it in the list of configurable packet-based flow sources.

When you configure the **Network Interface** flow source, configure only one log source for each Ethernet interface. To filter the network traffic that comes in on the flow source, specify a Berkeley Packet Filter (BPF) in the **Filter String** field.

After the flow source is configured and the changes are deployed, you can view the network traffic on the **Network Activity** tab.

You can customize the way that QRadar processes the network traffic. For example, you can configure the way that applications are detected, superflow thresholds, flow direction configuration, and network hierarchy. You can also write rules, perform queries, and filter the network traffic.

For more information, see Adding or editing a flow source and Configuring a flow collector in the IBM Knowledge Center.

Related tasks
Configuring a flow collector
Related information
Adding or editing a flow source

Flow aggregation

IBM QRadar combines information together to give you more information about a single flow without sending more flow records. This process is known as aggregation.

The flow shows a communication session between two hosts by normalizing the packet attributes into a flow record that includes the following information:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol
- Flow ID (flow source dependent)
- VLAN fields (flow source dependent)
- VXLAN fields (flow source dependent)

As the hosts continue to communicate, information such as the byte and packet counters and the payload capture is aggregated into a single flow record. For communications that span more than 1 minute, QRadar reports on the current metrics for the flow at the end of each 1-minute interval. The entire communication session is represented by multiple flow records that have the same **First Packet Time**, but with incremental **Last Packet Time** values.

The flow information is updated if the attributes are the same. When one or more attributes change, the flow is assumed to be unique, and a new flow record is created.

Flow capacity limits

Flow capacity limits ensure that the QFlow process in IBM QRadar is not overloaded.

When the QFlow process receives more traffic than it can deal with, an overflow record is created for each protocol that is observed in the excess traffic. These records are easily identified because they have a source IP address of 127.0.0.4 and a destination IP address of 127.0.0.5.

For example, QRadar determines that the flow capacity limit of your Flow Collector is 100,000 flows. During a peak period, the appliance captures 120,000 flows in a one minute interval. The excess 20,000 flows are not parsed, but instead an overflow record is created for each protocol that is seen in the 20,000 flows. The overflow record includes byte and packet counters, but information such as source or destination IP addresses, ports, and payload capture is not collected and stored.

Flow capacity limits

Flow capacity is determined based on a number of different factors:

Deployment flow limit
This flow limit is based on the sum of all flow licenses across your deployment.

Hardware flow limit
The hardware flow limit is the recommended number of flows calculated based on the available CPUs and memory.

User flow limits
You can set the maximum number of flows that you want QRadar to process at one time.

If a user flow limit is set, it takes precedence over both the deployment flow limit and the hardware limit.

If no user limit is set, the minimum of either the hardware limit or the deployment limit is used.

Note: To ensure that you achieve the maximum benefit from your flows per minute (FPM) license, flow capacity limits are enforced after aggregation. Updates to existing flows within the 1-minute reporting interval do not contribute to your FPM license limit.

Flow direction

The QFlow process analyzes each flow to determine the direction of the network communication.

In some cases, the flow traffic is bidirectional where the client communicates with the server and the server responds to the client. In this scenario, both the client and the server operate as though they are the source and the other is the destination. To address this, QRadar sets the flow direction to ensure that the source and destination devices are reported consistently throughout the entire communication session. The flow data is normalized and all flows follow the same convention, where **Destination** always refers to the server, and **Source** always refers to the client.

To determine the flow direction, QRadar analyzes the flow to determine whether the source and destination ports match the list of common destination ports that are defined in the QRadar configuration. The flow direction is reversed when the following criteria is matched:

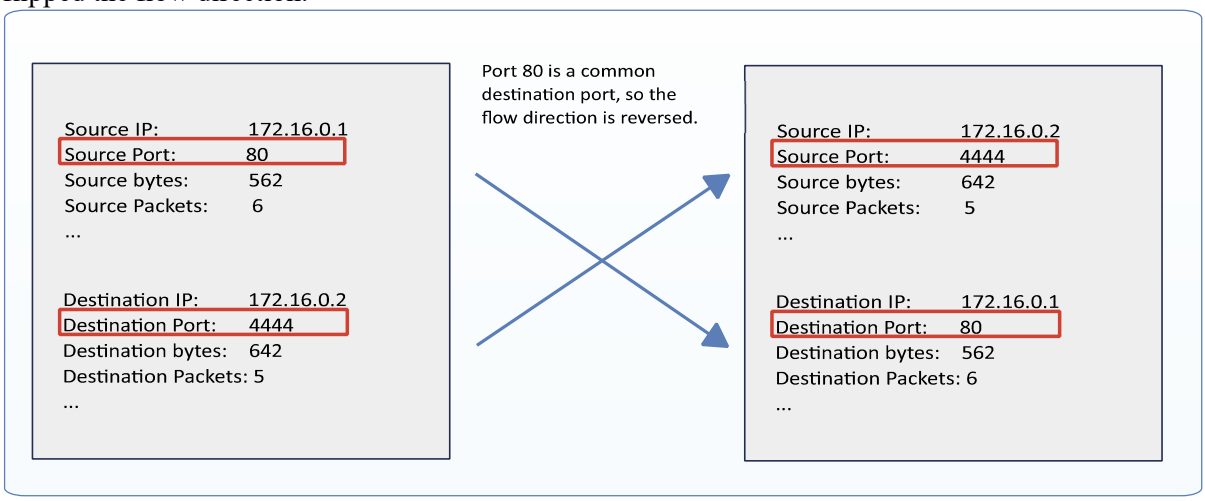
- If the destination port **does not** match the list of common destination ports, reverse the flow direction if **either** of the following conditions are true:
  - The source port is a common destination port.
  - The source port is less than 1024 and the destination port is greater than 1024.
- If the destination port **does** match the list of common destination ports, reverse the flow direction if **both** of the following conditions are true:
  - The source port is a common destination port.
  - The source port is less than 1024 and the destination port is greater than 1024.

If the flow does not match any of the flow direction criteria, QRadar uses the flow arrival time to determine the flow direction.

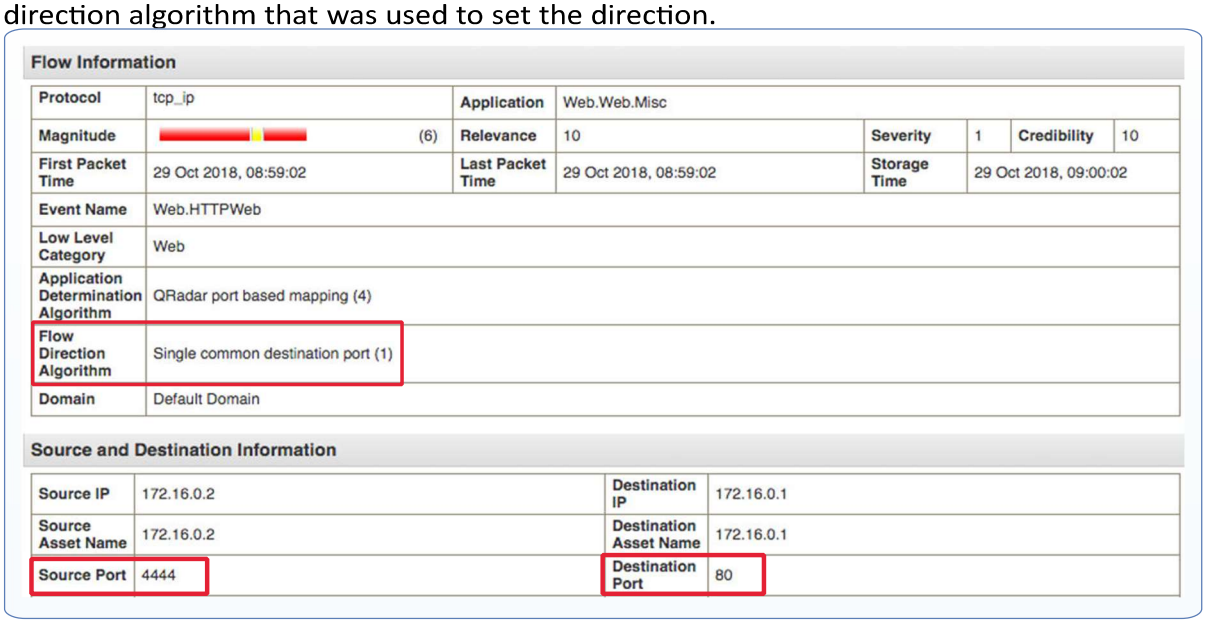
Tip: If you do not want QRadar to determine the flow direction, set the **Use Common Destination Port** field to **No** when you configure the Flow Collector. For more information, see "Configuring a flow collector" on page 105.

Example: Flow direction reversed by QRadar

In this flow, the source port is 80, which is a common destination port. The destination port is higher than 1024 which, according to RFC1700, excludes it as a common destination port. In this case, QRadar flipped the flow direction.



On the **Flow Information** window, you can see the flow direction algorithm that was used to set the direction.



Flow Information

Protocol	tcp_ip	Application	Web.Web.Misc				
Magnitude	(6)	Relevance	10	Severity	1	Credibility	10
First Packet Time	29 Oct 2018, 08:59:02	Last Packet Time	29 Oct 2018, 08:59:02	Storage Time	29 Oct 2018, 09:00:02		
Event Name	Web.HTTPWeb						
Low Level Category	Web						
Application Determination Algorithm	QRadar port based mapping (4)						
Flow Direction Algorithm	Single common destination port (1)						
Domain	Default Domain						

Source and Destination Information

Source IP	172.16.0.2	Destination IP	172.16.0.1
Source Asset Name	172.16.0.2	Destination Asset Name	172.16.0.1
Source Port	4444	Destination Port	80

Flow direction algorithms

Flow direction algorithms are used to detect which side of the communication is more likely to be the destination device, and reverses the flow direction as required. The algorithms provide information on how the traffic originally appeared on the network, and which features of the traffic caused it to be reversed.

The following table displays the values that are used in the flow direction algorithm.

Numeric value	Algorithm	Description
1	Changed in 7.4.2 Single common destination port (reversed)	Either the source port or the destination post was found in the list of common destination ports, and QRadar reversed the flow direction.

2	Changed in 7.4.2 Both common destination ports but one was RFC 1700 preferred (reversed)	Both the source port and the destination port are defined as common destination ports. According to RFC1700 (https://www.ietf.org/rfc/rfc1700.txt), the source port is a preferred destination port, so QRadar reversed the flow direction. The RFC1700 preferred ports are in the range of 0 to 1023, which are controlled and assigned by the Internet Assigned Number Authority (IANA).
3	Arrival time	The flow does not match the criteria for any other flow direction algorithm. QRadar used the flow arrival time to determine the flow direction. The QFlow process assumes that the request was received before the response, and the flow direction remains as it was received.
4	Flow exporter	The flow direction is set by an external flow exporter, such as a Packeteer device.
Numeric value	**Algorithm**	**Description**
5	New in 7.4.2 Single common destination port (unaltered)	Either the source port or the destination post was found in the list of common destination ports. QRadar did not alter the flow direction.
6	New in 7.4.2 Both common destination ports but one was RFC 1700 preferred (unaltered)	Both the source port and the destination port are defined as common destination ports. According to RFC1700 (https://www.ietf.org/rfc/rfc1700.txt), the destination port is a preferred destination port, so QRadar did not alter the flow direction.
7	New in 7.4.2 QNI TCP Handshake Observed (reversed)	IBM QRadar Network Insights observed a TCP handshake and determined that the flow direction should be reversed.
8	New in 7.4.2 QNI TCP Handshake Observed (unaltered)	IBM QRadar Network Insights observed a TCP handshake and determined that the flow direction should remain as it was observed.

Displaying the flow direction algorithm field in search results

Use the search feature to add the flow direction algorithm to the **Flow Details** window. You can use the flow direction algorithm to identify the criteria that caused QRadar to reverse the flow direction.

Procedure

1. To display the flow direction algorithm field on the **Flow Details** window, follow these steps: a) Click the **Network Activity** tab.
   b) From the **Search** list, select **New Search**.
   c) In the **Column Definition** section, scroll down the list of available columns and add **Flow Direction Algorithm** to the list of columns to display.
   d) Click **Filter**.

The **Flow Direction Algorithm** column appears on the **Network Activity** tab, displaying a value that represents the algorithm that was used.

2. To display the flow direction algorithm in an advanced search, use the LOOKUP function to show thetext description for the enumerated flow direction algorithm field. For example, the AQL query might look like this:

```
SELECT sourceip, destinationip, LOOKUP('flow direction algorithm', "flow direction algorithm") FROM flows
```

Common destination ports

New in 7.4.3

Common destination ports are used by QRadar to determine the direction of a network communication, and to ensure that the source and destination devices are reported consistently throughout the entire communication session.

Use the Common Destination Ports API to view the common destination ports that are configured in your system, and add new common destination ports.

Note: Earlier versions of QRadar used the appid_map.conf configuration file to determine the list of common destination ports.

You can use the Common Destination Port API to do the following actions:

- Get a list of the common destination ports that are defined by default.

  config/flow/applications/common_destination_ports/default_configurations

  The default configurations are read-only. They are provided as a system backup in case the configuration is mistakenly deleted or changed.
- Get information about the common destination ports that are active in the deployed system. Thisendpoint is also used to create, update, or delete active common destination ports.

  config/flow/applications/common_destination_ports/active_configurations

  When you use the API to change the common destination ports, the QFlow process automatically loads the configuration. You do not need to deploy the configuration to propagate the changes to the system.

For more information about using the QRadar RESTful API, see RESTful API overview.

Application identification

The QFlow process uses algorithms to determine the flow application. Each algorithm relies on different types of information to determine the application.

IBM QRadar Network Insights relies on its own set of inspectors and deeper application detection methods.

The application determination algorithms are shown in the following table:

Table 17. Application determination algorithms

Numeric value	Algorithm name	Description

2	Application signatures	A payload-based algorithm that looks at the way that the payload is structured. This algorithm uses information from the signatures.xml file.
3	State-based decoding	A payload-based algorithm that uses complex internal logic.
4	QRadar port-based mapping	A port-based algorithm that uses a pre-defined list of application mappings. This algorithm uses information from the /opt/qradar/conf/appid_map.conf file.
5	User port-based mapping	A port-based algorithm that uses a customizable list of application mappings. Use this algorithm to add new port-based mappings or reclassify existing mappings that come with QRadar. This algorithm uses information from the /opt/qradar/conf/user_application_mapping.conf file.
6	ICMP protocol mapping	A protocol-based algorithm that looks at the protocol type and code.

Table 17. Application determination algorithms (continued)

Numeric value	**Algorithm name**	**Description**
7	Flow exporter	An algorithm that relies on the Flow Exporter to determine the application. For example, the QFlow process inherently trusts application IDs that come from QRadar Network Insights.
8	QNI Application Signatures	This algorithm is used by IBM QRadar Network Insights.
9	QNI Inspectors	This algorithm is used by IBM QRadar Network Insights.
10	X-Force Web Application Classification	This algorithm is used by IBM QRadar Network Insights.

You can see which type of application detection algorithm that QRadar used in the **Application Determination Algorithm** field on the **Flow Information** window.

Flow Information

Protocol	tcp_ip	**Application**	Web.Web.Misc				
Magnitude	(6)	**Relevance**	10	**Severity**	1	**Credibility**	10
First Packet Time	29 Oct 2018, 08:59:02	**Last Packet Time**	29 Oct 2018, 08:59:02	**Storage Time**	29 Oct 2018, 09:00:02		
Event Name	Web.HTTPWeb						
Low Level Category	Web						
Application Determination Algorithm	QRadar port based mapping (4)						
Flow Direction Algorithm	Single common destination port (1)						
Domain	Default Domain						

Source and Destination Information

Source IP	172.16.0.2	**Destination IP**	172.16.0.1
Source Asset Name	172.16.0.2	**Destination Asset Name**	172.16.0.1
Source Port	4444	**Destination Port**	80

Custom applications

If your organization has non-standard or customized applications, you can add them to the /opt/qradar/conf/user_application_mapping.conf or signatures.xml files.

You can use the **Application Determination Algorithm** field to check that the correct algorithm was used to identify your customized applications. For example, you might define a custom application based on the port usage. Flows from that application are identified by algorithm 5, which is **User Port Based Mapping**. By verifying the algorithm that is used to identify the application, you can assign a level of confidence to the application mapping.

For more information, see the *IBM QRadar Application Configuration Guide*.

Displaying the application determination algorithm field in search results

Use the search feature to add the application determination algorithm to the **Flow Details** window. You can use the application identification algorithm to identify the criteria that QRadar used to identify which application the flow originated from.

Procedure

1. To display the application determination algorithm field on the **Flow Details** window, follow these steps:
   a) Click the **Network Activity** tab.
   b) From the **Search** list, select **New Search**.
   c) In the **Column Definition** section, scroll down the list of available columns and add **Application Determination Algorithm** to the list of columns to display.
   d) Click **Filter**.
   The **Application Determination Algorithm** column appears on the **Network Activity** tab, displaying a value that represents the algorithm that was used.
2. To display the application determination algorithm in an advanced search, use the LOOKUP function toshow the text description for the enumerated algorithm field. For example, the AQL query might look like this.

```
SELECT LOOKUP('application determination algorithm', "application determination algorithm"),
* FROM flows
```

Superflows

IBM QRadar analyzes individual flows to look for indicators that common attack vectors are being used on your network. When the number of flows that match the criteria reaches a specified number, QRadar groups the individual flows into a *superflow*. Each superflow counts as only one flow against the flows per minute (FPM) license, regardless of how many flow records are bundled within it.

You can configure the flow threshold to control the number of unique flows that must match the criteria before a superflow is created. Given a threshold of 100, the first 99 flows are sent as normal flow records. The 100th flow and subsequent matching flows are included in the superflow record. QRadar continues to report on the superflow every minute until one full interval passes with no matching traffic. Because a superflow is kept alive even if only one flow record matches, some superflows might appear to be small.

Tip: If you do not want QRadar to create superflows, in the Flow Collector configuration settings, change the **Create Super Flows** setting to No.

Superflow Type A: Network scan

A network scan attempts to discover all of the active hosts on your network and map the hosts to an IP address.

QRadar looks for flows where one host sends data to many hosts, and flags this type of activity as a Type A superflow. This unidirectional flow is an aggregate of all of the flows that have the same source IP with different destination IPs, but the following parameters are the same:

- Protocol
- Source bytes-to-packets ratio
- Source IP address
- Destination port (TCP and UDP flows only)
- TCP flags (TCP flows only)
- ICMP type and code (ICMP flows only)

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
A	8 Apr 2016, 06:32:26	10.91.229.20	N/A	Multiple (9)	N/A	icmp_ip
A	8 Apr 2016, 06:32:25	10.91.229.20	N/A	Multiple (5)	N/A	icmp_ip
A	8 Apr 2016, 06:32:26	10.104.8.249	Multiple (6)	Multiple (6)	47808	udp_ip
A	8 Apr 2016, 06:32:49	10.91.229.20	N/A	10.104.8.58	N/A	icmp_ip
A	8 Apr 2016, 06:32:36	10.112.38.51	Multiple (13)	Multiple (13)	53213	udp_ip
A	8 Apr 2016, 06:32:59	10.106.168.37	Multiple (3)	Multiple (3)	8612	udp_ip
A	8 Apr 2016, 06:32:57	10.106.168.37	Multiple (2)	Multiple (2)	8612	udp_ip

Superflow Type B: Distributed denial of service (DDoS)

A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system.

QRadar looks for flows where many hosts send data to one destination host, and flags this activity as a Type B superflow. This unidirectional flow is an aggregate of all of the flows that have different source IPs with a single destination IP, but the following parameters are the same:

- Protocol
- Source bytes-to-packets ratio
- Destination IP address
- Destination port (TCP and UDP flows only)

- TCP flags (TCP flows only)
- ICMP type and code (ICMP flows only)

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
B	8 Apr 2016, 06:32:34	Multiple (64)	Multiple (64)	10.92.229.21	137	udp_ip
B	8 Apr 2016, 06:32:32	Multiple (68)	Multiple (68)	10.91.229.21	137	udp_ip
B	8 Apr 2016, 06:32:54	Multiple (3)	Multiple (3)	10.92.229.20	137	udp_ip
B	8 Apr 2016, 06:32:54	Multiple (4)	Multiple (4)	10.91.229.20	137	udp_ip
B	8 Apr 2016, 06:32:35	Multiple (53)	Multiple (53)	10.92.229.21	137	udp_ip
B	8 Apr 2016, 06:32:32	Multiple (52)	Multiple (52)	10.91.229.21	137	udp_ip
B	8 Apr 2016, 06:32:36	Multiple (27)	Multiple (27)	10.91.0.60	80	tcp_ip
B	8 Apr 2016, 06:33:20	Multiple (3)	Multiple (3)	10.92.229.21	137	udp_ip

Superflow Type C: Port scan

A port scan attempts to identify the ports that are in use by a specific host on your network.

QRadar looks for flows that have one source IP and one destination IP, but many ports. This unidirectional flow is an aggregate of all non-ICMP flows that have different source or destination ports, but the following parameters are the same:

- Protocol
- Source IP address
- Destination IP address
- Source bytes-to-packets ratio
- TCP flags (TCP flows only)

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
C	8 Apr 2016, 06:32...	10.91.229.20	Multiple (2)	10.103.24.38	Multiple (2)	tcp_ip
C	8 Apr 2016, 06:32...	10.89.2.34	Multiple (2)	10.89.160.4	Multiple (2)	tcp_ip
C	8 Apr 2016, 06:32...	10.89.2.34	Multiple (3)	10.89.160.1	Multiple (3)	tcp_ip
C	8 Apr 2016, 06:32...	10.89.162.1	Multiple (12)	10.89.2.11	Multiple (12)	udp_ip
C	8 Apr 2016, 06:33...	10.89.2.24	Multiple (5)	10.202.32.116	Multiple (5)	tcp_ip
C	8 Apr 2016, 06:33...	10.89.2.34	Multiple (5)	10.89.160.2	Multiple (5)	tcp_ip

Deduplication

If your IBM QRadar deployment includes multiple Flow Collectors that provide data to a Flow Processor, you can configure flow deduplication to remove duplicate flows. The flow deduplication process ensures that flow records with the same unique identifier are reported only once.

Before discarding the duplicate flow, QRadar merges the following fields with the original flow record so that you can tell where the duplicate record was observed on the network.

- Flow source ID
- Flow source name
- Source ASN
- Destination ASN
- Input IF index
- Output IF index

Configuring flow deduplication

You can configure flow deduplication to take place at either the Flow Collector or the Flow Processor.

When your Flow Collector receives data from two different flow sources that are monitoring the same part of the network, configure deduplication at the Flow Collector appliance. For example, your Flow Collector might receive data from a 3rd party flow exporter as well as its own network TAP.

When you have two different Flow Collectors that monitor overlapping parts of the network, the individual flow collectors are unaware of the deduplication. In the scenario, you configure deduplication at the Flow Processor appliance.

You can set the flow deduplication method in the configuration settings for the appliance. For more information, see "Configuring a flow collector" on page 105.

View flow data on the Network Activity tab

The default view on the **Network Activity** tab is a stream of real-time events. As the hosts continue to communicate, the flow is updated. The entire communication session is represented by multiple flow records that have the same **First Packet Time**, but with **Last Packet Time** values that increment through time.

The **View** list contains options to also view events for specified time periods. After you choose a specified time period from the **View** list, you can modify the displayed time period by changing the date and time values in the Start Time and End Time fields.

Viewing normalized flow data

Normalization involves preparing flow data to display readable information. You view normalized flow data on the **Network Activity** tab.

Procedure

1. Click the **Network Activity** tab.
2. In the center of the window, from the **Display** list box, choose the display view that you want to see.

   The **Normalized (With IPv6 Columns)** display shows source and destination IPv6 addresses for IPv6 flows.
3. From the **View** list box, select the time frame that you want to display.
   a) To stream flows as they are received, select **Real Time**.

      You can click the **Pause** icon to pause streaming.
   b) To reduce the number of flows that you see, select a time frame.

      If you select a time frame to display, a time series chart is displayed. Click **Hide Charts** to remove it. If you use the Mozilla Firefox web browser and you have an ad blocker extension installed, the charts do not appear.

      For more information about using time series charts, see Time series chart overview.
4. To view the more information about a particular flow, double-click it to open the **Flow Information** window.

Viewing streaming flows

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

About this task

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

Procedure

1. Click the **Network Activity** tab.
2. From the View list box, select **Real Time (streaming)**.
3. Optional. Pause or play the streaming flows. When streaming is paused, the last 1,000 flows aredisplayed.

   Note: When you are streaming flows, the status bar displays the average number of results that are received per second. This display is the number of results that the Console successfully received from the Flow 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, hover over the status bar.

   When flows are not streaming, the status bar displays the number of search results that are currently displayed and the amount of time that is required to process the search results.

Viewing grouped flows

View flows that are grouped by various options.

About this task

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

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 flows table represents a flow group.

Procedure

1. Click the **Network 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 flows on.
4. To view the **List of Flows** page for a group, double-click the flow group that you want to investigate.

   The **List of Flows** page does not retain chart configurations that you might define on the **Network Activity** tab.
5. To view the details of a flow, double-click the flow that you want to investigate.

Viewing AWS flow log data

Flow logs that are received through Amazon Web Service (AWS) integrations include extra properties in the flow information.

About this task

In addition to the standard normalized flow properties, the following properties are shown for AWS flow logs:

- Interface name (available for all IPFIX flows that send this field)
- Region (available for all IPFIX flows that send this field)
- Firewall Name (available for all IPFIX flows that send this field)

- Firewall Event (enumerated, available for all IPFIX flows that send this field)
- AWS Action (enumerated)
- AWS Log Status (enumerated)• AWS Account ID

The following table shows the string description for each of the enumerated fields:

Table 18. AWS Enumerated Strings	
Enumerated field	**String description**
Firewall Event	The numerical values for the **Firewall Event** field map to the following descriptions: • 0 = Ignore • 1 = Flow Created • 2 = Flow Deleted • 3 = Flow Denied • 4 = Flow Alert • 5 = Flow Update
Table 18. AWS Enumerated Strings (continued)	
Enumerated field	**String description**
AWS Action	The numerical values for the **AWS Action** field map to the following descriptions: • 0 = N/A • 1 = Accept • 2 = Reject
AWS Log Status	The numerical values for the **AWS Log Status** field map to the following descriptions: • 0 = N/A • 1 = OK • 2 = No Data • 3 = Skip Data

Procedure

To include the description for the enumerated property in your query results, you must include the LOOKUP function in your AQL search string.

a) Click the **Network Activity** tab.

b) In the **Advanced Search** box, build the AQL query that includes the LOOKUP for the field that you want to include in your search.

The following examples show the LOOKUP statements for each of the enumerated fields in the AWS flow log:

```
LOOKUP('firewall event', "firewall event")

LOOKUP('aws action', "aws action")

LOOKUP('aws log status', "aws log status")
```

For example, the following query uses a LOOKUP in the WHERE clause and groups the accepted flows by application:

```
SELECT APPLICATIONNAME(applicationid), count(*) as NumFlows FROM flows
WHERE LOOKUP('aws action', "aws action") == 'Accept'
GROUP BY applicationid ORDER BY NumFlows DESC
```

In this example, the query uses a LOOKUP in the SELECT clause to show the number of accepted flows vs rejected flows in the AWS environment:

```
SELECT LOOKUP('aws action', "aws action"), count(*) as NumFlows
FROM flows WHERE "aws action" > 0 GROUP BY "aws action"
ORDER BY NumFlows DESC LAST 7 DAYS
```

Viewing flows that contain MPLS fields

Internet Protocol Flow Information Export (IPFIX) is a common protocol that allows exporting of flow information from network devices. Multiprotocol Label Switching (MPLS) is a routing technique that runs on any protocol.

With MPLS support for IPFIX flow records in QFlow, you can filter and search for IPFIX flows in IBM QRadar that contain MPLS fields and write rules based on the values of these MPLS fields.

For example, an IPFIX flow is exported from a switch on a network that uses MPLS. The IPFIX flow that is exported from the router contains information about the MPLS stack, which is now saved as part of the flow in QRadar®. The MPLS stack can contain up to 10 layers where each layer shows information about the flow routing. These MPLS fields are included in rules, searches, and filters, and can be viewed in the **Flow Details** window.

Filter on MPLS fields

Use the **Add Filter** option on the **Network Activity** tab to filter on MPLS fields.

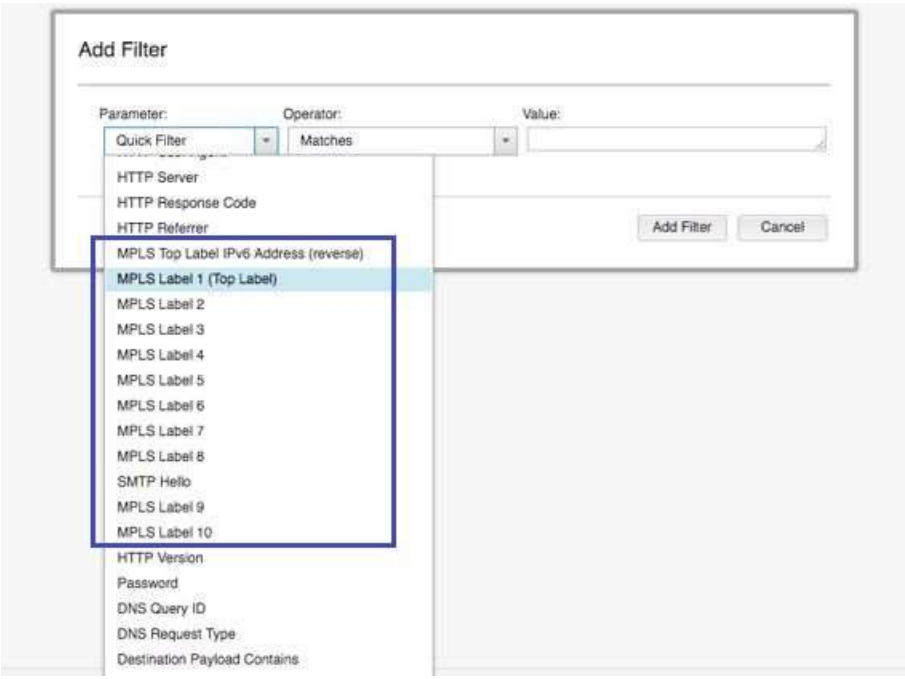


Figure 7. Filter on MPLS fields

Search for MPLS fields

Use the **Advanced Search** option on the **Network Activity** tab to search for MPLS fields.

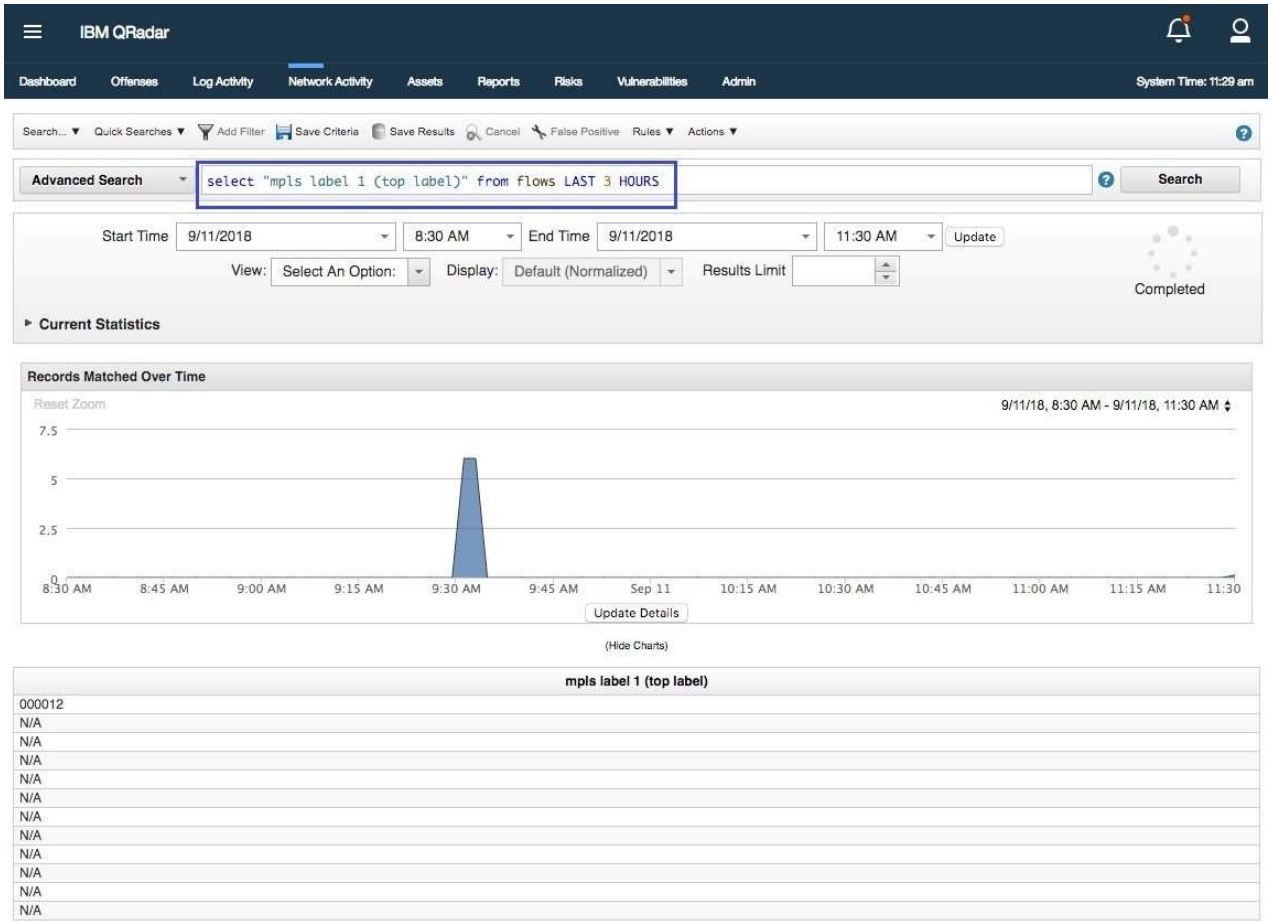


Figure 8. Search for MPLS fields

For more information about using the **Advanced Search** option, see Advanced search options.

View information about MPLS fields

You can view information about MPLS fields by double-clicking a flow in the **Flow Details** window on the **Network Activity** tab.

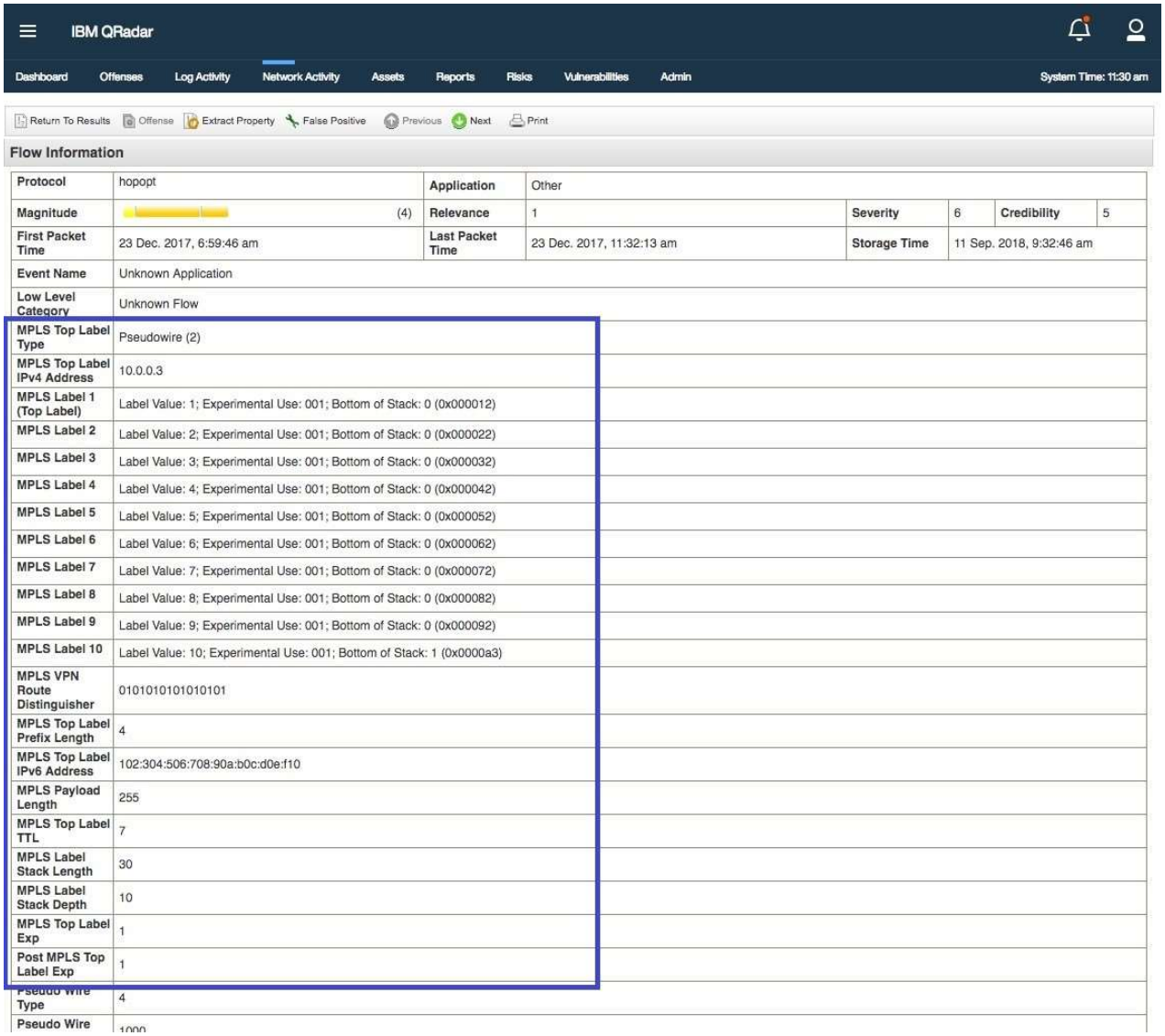


Figure 9. MPLS fields in Flow Information

IPFIX MPLS information elements

The following table describes the IPFIX MPLS information elements that are supported. All of these elements have Private Enterprise Number (PEN): 0.

Field	Element ID
mplsTopLabelType	46
mplsTopLabelIPv4Address	47
mplsTopLabelStackSection	70
mplsLabelStackSection2	71
mplsLabelStackSection3	72

mplsLabelStackSection4	73
mplsLabelStackSection5	74
mplsLabelStackSection6	75
Field	**Element ID**
mplsLabelStackSection7	76
mplsLabelStackSection8	77
mplsLabelStackSection9	78
mplsLabelStackSection10	79
mplsVpnRouteDistinguisher	90
mplsTopLabelPrefixLength	91
mplsTopLabelIPv6Address	140
mplsPayloadLength	194
mplsTopLabelTTL	200
mplsLabelStackLength	201
mplsLabelStackDepth	202
mplsTopLabelExp	203
postMplsTopLabelExp	237
pseudoWireType	250
pseudoWireControlWord	251
mplsLabelStackSection	316
mplsPayloadPacketSection	317
sectionOffset	409
sectionExportedOctets	410

For more information about each field, see the IANA information element assignment at IP Flow Information Export (IPFIX) Entities (https://www.iana.org/assignments/ipfix/ipfix.xhtml).

Exporting flows

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

Procedure

1. Click the **Network Activity** tab.
2. Optional. If you are viewing flows 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 flow 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 flow parameters. A full export can take an extended period of time to complete.
4. If you want to resume your activities, 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.

VLAN fields

QRadar retains Virtual Local Area Network (VLAN) information that is exported in external flow records, such as those that are received from IPFIX, NetFlow V9, sFlow V5, or J-Flow V9. VLAN can also be viewed in internal flows, such as those that are received by Napatech or Network Interface Cards, or a dedicated IBM QRadar Network Insights appliance. You can then query, filter, search, or write custom rules with this VLAN information.

The following VLAN fields are supported for IPFIX, Netflow version 9, and J-Flow.

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI (raw packets only)
- dot1qCustomerDEI (raw packets only)

The following VLAN fields are supported for raw packets and sFlow version 5.

- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- dot1qDEI

- dot1qCustomerDEI

All flows with VLAN information contain two IBM-specific fields that can be used to define unique domains in QRadar:

- Enterprise VLAN ID
- Customer VLAN ID

For example, a UDP flow is sent from 10.0.0.1:123 to 10.0.0.2:456 on VLAN 10. Another UDP flow is sent from 10.0.0.1:123 to 10.0.0.2:456 on VLAN 20. In QRadar, the unique identifier for each flow includes the nested VLAN fields (including **post** fields). This means that the two flows above are treated independently, each with their own VLAN definition.

Assign domains and tenants to flows with VLAN information

With domain management support for VLAN flows, you can define your domains in QRadar based on the VLAN information in your network.

In QRadar, you can assign domains to incoming flows based on the VLAN information that is contained in the flow. The incoming flows are mapped to domains that contain the same VLAN definition. You can also filter and query the domains for the VLAN-based domain.

You can assign tenants to domain definitions to achieve multi-tenancy. The VLAN-based domain definitions enable multi-tenancy across different VLANs, if required.

For example, two domain definitions are created and mapped to two network tenants:

- For *tenant ABC*, traffic is sent on Enterprise VLAN ID = 0, and Customer VLAN ID = 10.
- For *tenant DEF*, traffic is sent on Enterprise VLAN ID = 0, and Customer VLAN ID = 20.

The first domain definition is created for *tenant ABC*, which contains a flow VLAN definition of Enterprise VLAN ID = 0 and customer VLAN ID = 10.

A second domain definition is created for *tenant DEF*, which contains a flow VLAN definition of Enterprise VLAN ID = 0 and customer VLAN ID = 20.

Incoming flows with Enterprise VLAN ID and Customer VLAN ID fields set to 0 and 10 are viewed only by *tenant ABC*. Similarly, incoming flows with Enterprise VLAN ID and Customer VLAN ID fields of 0 and 20 are only viewed by *tenant DEF*. This reflects the traffic ownership for each tenant in the network.

Configuring a flow collector

By changing the Flow Collector configuration settings, you can manage the way that IBM QRadar collects and processes flows that are received from the device.

The following table describes the Flow Collector configuration parameters:

Table 19. Flow collector configuration parameters

Parameter	**Description**
Maximum Content Capture	Specify the maximum amount of data (bytes per packet) that you want the Flow Collector to capture and retain in the flow payload.

Maximum Data Capture/Packet	Specify the maximum amount of data (bytes per packet) that you want the Flow Collector to analyze.
Flow buffer size	Specify the maximum number of flows that can be buffered in memory.
Maximum Number of Flows	Specify the maximum number of flows that you want to send from the Flow Collector to an Event Collector within a 1 minute interval.
Alias Autodetection	Set to **Yes** to allow QRadar to auto-detect flow sources. With auto-detection turned on, QRadar can automatically create flow source aliases for external flow sources, such as routers.
Remove duplicate flows	Set this to **Yes** if you want the Flow Collector to remove duplicate flows. If you have asymmetric traffic in your network, set this parameter to **No**.
Verify NetFlow Sequence Numbers	Set this to **Yes** if you want the Flow Collector to check the incoming NetFlow sequence numbers to ensure that all packets are present and in order. QRadar displays a notification if a packet is missing or received in incorrect sequence.

Table 19. Flow collector configuration parameters (continued)

Parameter	**Description**
External Flow De-duplication method	Choose the method that you want to use to remove duplicate external flows. • Select **Source** to compare the originating flow sources. This method compares the IP address of the device that exported the current external flow record to the IP address of the device that exported the first external record of the flow. If the IP addresses do not match, the current external flow record is discarded. • Select **Record** to compare the individual external flow records. This method logs a list of every external flow record that is detected by a device, and compares each subsequent record to that list. If the current record is found in the list, the record is discarded. If you choose this method, you must also set the **External flow record comparison mask** parameter.

Flow Carry-over Window	Specify the number of seconds that the QFlow process holds onesided flows. The default setting is 6 seconds. This setting allows time for QRadar to receive the flow response. Flows that fall within the carry-over window are not sent until the next reporting interval.
External flow record comparison mask	Specify the method to use to compare external flow records. This parameter is valid only if you chose **Record** as the method to use for external flow De-duplication. You can choose which flow record fields are to be used when comparing external flow records: • D (Direction) • B (ByteCount) • P (PacketCount) You can combine the flow record fields to include the following combinations: • The **DBP** option uses direction, byte count, and packet count. • The **XBP** option uses byte count and packet count. • The **DXP** option uses direction and packet count. • The **DBX** option uses direction and byte count. • The **DXX** option uses direction. • The **XBX** option uses byte count. • The **XXP** option uses packet count.
Create Super Flows	Set this to **Yes** if you want QRadar to group flows that have similar properties into one flow record
Type A Superflows (Network Scan)	Specify the threshold to be reached before QRadar creates a Type A (one to many) superflow.

Table 19. Flow collector configuration parameters (continued)

Parameter	**Description**
Type B Superflows (DDos)	Specify the threshold to be reached before QRadar creates a Type B (many to one) superflow.
Type C Superflows (Port Scan)	Specify the threshold to be reached before QRadar creates a Type C (one to one) superflow.
Recombine Asymmetric flows	Set this to **Yes** if you want QRadar to recombine asymmetric flows.
Ignore Asymmetric Superflows	Set this to **Yes** if you want QRadar to create superflows when asymmetric flows are enabled.
Use Common Destination Port	Set this to **Yes** if you want QRadar to determine whether to reverse the flow direction.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**, and select the Flow Collector that you want to configure.
4. On the **Deployment Actions** menu, click **Edit Host**.
5. Click the gear icon next to **Component Management**.
6. Edit the configuration options and click **Save**.
7. Repeat the configuration steps for each Flow Collector in your deployment.
8. Close the **System and License Management** window.
9. Deploy your changes.
   This will restart the QFlow process on every managed host that you modified.

Related concepts
NetFlow IPFIX
sFlow J-Flow
Packeteer Napatech
interface
If you installed a Napatech Network Adapter on your IBM QRadar system, you can monitor the packets that the card sees. The Napatech card must be installed for QRadar to show it in the list of configurable packet-based flow sources.

Network interface
IBM QRadar can monitor packets that come in on any network interface card that is installed on your system. The network interface card must be installed for QRadar to show it in the list of configurable packet-based flow sources.

Tuning false positive events from creating offenses

You can prevent false positive flows from creating offenses. You can tune false positive flows from the flow list or flow details page.

About this task

You must have appropriate permissions for creating customized rules to tune false positives.

Procedure

1. Click the **Network Activity** tab.
2. Optional. If you are viewing flows in streaming mode, click the **Pause** icon to pause streaming.
3. Select the flow that you want to tune.
4. Click **False Positive**.
5. In the Event/Flow Property pane on the **False Positive** page, select one of the following options:
   - Event/Flow(s) with a specific QID of <Event>
   - Any Event/Flow(s) with a low-level category of <Event>
   - Any Event/Flow(s) with a high-level category of <Event>
6. In the Traffic Direction pane, select one of the following options:
   - <Source IP Address> to <Destination IP Address>
   - <Source IP Address> to any Destination

- Any Source to <Destination IP Address>
- Any Source to any Destination

7. Click **Tune**.

Chapter 8. Asset Management

Collecting and viewing asset data helps you to identify threats and vulnerabilities. An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network.

Restriction: QRadar Log Manager only tracks asset data if QRadar Vulnerability Manager is installed. For more information about the differences between IBM QRadar SIEM and IBM QRadar Log Manager, see Chapter 2, "Capabilities in your IBM QRadar product," on page 5.

Asset data

An *asset* is any network endpoint that sends or receives data across your network infrastructure. For example, notebooks, servers, virtual machines, and handheld devices are all assets. Every asset in the asset database is assigned a unique identifier so that it can be distinguished from other asset records.

Detecting devices is also useful in building a data set of historical information about the asset. Tracking asset information as it changes helps you monitor asset usage across your network.

Asset limits

The asset database has a limited capacity. When the asset limit for your hardware is reached, you cannot create any new assets until sufficient space is available in the database. The following table describes the asset limits for each hardware type:

Table 20. Asset limits for hardware

Hardware type	Asset Limit for Console only	Asset Limit for Console with Managed Host
xx05	200,000	600,000
xx24	300,000	700,000
xx28	500,000	1,000,000
xx29	500,000	1,000,000
xx48	500,000	1,000,000
Other hardware	60,000	60,000

Asset profiles

An *asset profile* is a collection of all information that IBM QRadar SIEM collected over time about a specific asset. The profile includes information about the services that are running on the asset and any identity information that is known.

QRadar SIEM automatically creates asset profiles from identity events and bidirectional flow data or, if they are configured, vulnerability assessment scans. The data is correlated through a process that is called *asset reconciliation* and the profile is updated as new information comes into QRadar. The asset name is derived from the information in the asset update in the following order of precedence:

- Given name

- NETBios host name
- DNS host name
- IP address

© Copyright IBM Corp. 2012, 2021

Collecting asset data

Asset profiles are built dynamically from identity information that is passively absorbed from event or flow data, or from data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually.

Sources of asset data

Asset data is received from several different sources in your IBM QRadar deployment.

Asset data is written to the asset database incrementally, usually 2 or 3 pieces of data at a time. With exception of updates from network vulnerability scanners, each asset update contains information about only one asset at a time.

Asset data usually comes from one of the following asset data sources:

Events

Event payloads, such as those created by DHCP or authentication servers, often contain user logins, IP addresses, host names, MAC addresses, and other asset information. This data is immediately provided to the asset database to help determine which asset the asset update applies to.

Events are the primary cause for asset growth deviations.

Flows

Flow payloads contain communication information such as IP address, port, and protocol that is collected over regular, configurable intervals. At the end of each interval, the data is provided to the asset database, one IP address at a time.

Because asset data from flows is paired with an asset based on a single identifier, the IP address, flow data is never the cause of asset growth deviations.

Important: Asset generation from IPv6 flows is not supported.

Vulnerability scanners

QRadar integrates with both IBM and third-party vulnerability scanners that can provide asset data such as operating system, installed software, and patch information. The type of data varies from scanner to scanner and can vary from scan to scan. As new assets, port information, and vulnerabilities are discovered, data is brought into the asset profile based on the CIDR ranges that are defined in the scan.

It is possible for scanners to introduce asset growth deviations but it is rare.

User interface

Users who have the Assets role can import or provide asset information directly to the asset database. Asset updates that are provided directly by a user are for a specific asset. Therefore the asset reconciliation stage is bypassed.

Asset updates that are provided by users do not introduce asset growth deviations.

Domain-aware asset data

When an asset data source is configured with domain information, all asset data that comes from that data source is automatically tagged with the same domain. Because the data in the asset model is domain-aware, the domain information is applied to all QRadar components, including identities, offenses, asset profiles, and server discovery.

When you view the asset profile, some fields might be blank. Blank fields exist when the system did not receive this information in an asset update, or the information exceeded the asset retention period. The default retention period is 120 days. An IP address that appears as 0.0.0.0 indicates that the asset does not contain IP address information.

Incoming asset data workflow

IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Important: Asset generation from IPv6 flows is not supported.

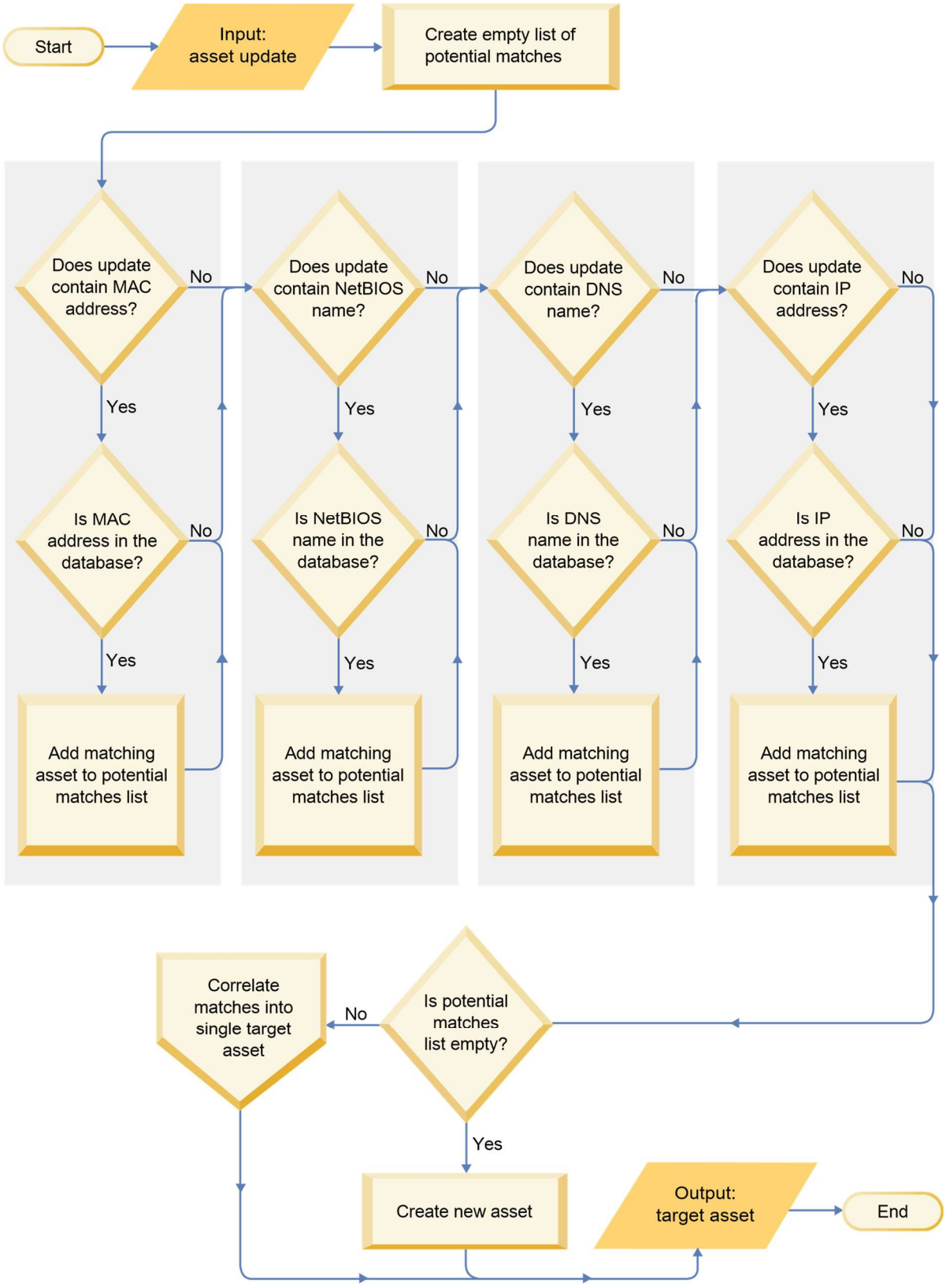


Figure 10. Asset data workflow diagram

1. QRadar receives the event. The asset profiler examines the event payload for identity information.

2. If the identity information includes a MAC address, a NetBIOS host name, or a DNS host name thatare already associated with an asset in the asset database, then that asset is updated with any new information.
3. If the only available identity information is an IP address, the system reconciles the update to theexisting asset that has the same IP address.
4. If an asset update has an IP address that matches an existing asset but the other identity informationdoes not match, the system uses other information to rule out a false-positive match before the existing asset is updated.
5. If the identity information does not match an existing asset in the database, then a new asset iscreated based on the information in the event payload.

Updates to asset data

IBM QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Each asset update must contain trusted information about a single asset. When QRadar receives an asset update, the system determines which asset to which the update applies.

Asset reconciliation is the process of determining the relationship between asset updates and the related asset in the asset database. Asset reconciliation occurs after QRadar receives the update but before the information is written to the asset database.

Identity information

Every asset must contain at least one piece of identity data. Subsequent updates that contain one or more pieces of that same identity data are reconciled with the asset that owns that data. Updates that are based on IP addresses are handled carefully to avoid false-positive asset matches. False positive asset matches occur when one physical asset is assigned ownership of an IP address that was previously owned by another asset in the system.

When multiple pieces of identity data are provided, the asset profiler prioritizes the information from the most deterministic to the least in the following order:

- MAC address
- NetBIOS host name
- DNS host name
- IP address

MAC addresses, NetBIOS host names, and DNS host names are unique and therefore are considered as definitive identity data. Incoming updates that match an existing asset only by the IP address are handled differently than updates that match more definitive identity data.

Related concepts
Asset reconciliation exclusion rules

Asset reconciliation exclusion rules

With each asset update that enters IBM QRadar, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

By default, each piece of asset data is tracked over a two-hour period. If any one piece of identity data in the asset update exhibits suspicious behavior two or more times within 2 hours, that piece of data is added to the asset blacklists. Each type of identity asset data that is tested results in a new blacklist.

Tip: QRadar excludes events based on data that is received in the event, not on any data that is later inferred or linked to the event.

In domain-aware environments, the asset reconciliation exclusion rules track the behavior of asset data separately for each domain.

The asset reconciliation exclusion rules test the following scenarios:

Table 21. Rule tests and responses

Scenario	Rule response
When a MAC address is associated to three or more different IP addresses in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When a DNS host name is associated to three or more different IP addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a DNS host name is associated to three or more different MAC addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When an IPv4 address is associated to three or more different DNS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a MAC address is associated to three or more different DNS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When an IPv4 address is associated to three or more different NetBIOS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a DNS host name is associated to three or more different NetBIOS host names in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a MAC address is associated to three or more different NetBIOS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist

You can view these rules on the **Offenses** tab by clicking **Rules** and then selecting the **asset reconciliation exclusion** group in the drop-down list.

Related concepts

Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

As the Network security administrator, you manage a corporate network that includes a public wifi network segment where IP address leases are typically short and frequent. The assets on this segment of the network tend to be transient, primarily notebooks and hand-held devices that log in and out of the public wifi frequently. Commonly, a single IP address is used multiple times by different devices over a short time.

In the rest of your deployment, you have a carefully managed network that consists only of inventoried, well-named company devices. IP address leases are much longer in this part of the network, and IP addresses are accessed by authentication only. On this network segment, you want to know immediately when there are any asset growth deviations and you want to keep the default settings for the asset reconciliation exclusion rules.

Blacklisting IP addresses

In this environment, the default asset reconciliation exclusion rules inadvertently blacklist the entire network in a short time.

Your security team finds the asset-related notifications that are generated by the wifi segment are a nuisance. You want to prevent the wifi from triggering any more deviating asset growth notifications.

Tuning asset reconciliation rules to ignore some asset updates

You review the **Asset deviation by log source** report in the last system notification. You determine that the blacklisted data is coming from the DHCP server on your wifi.

The values in the **Event Count** column, **Flow Count** column and the **Offenses** column for the row corresponding to the **AssetExclusion: Exclude IP By MAC Address** rule indicate that your wifi DHCP server is triggering this rule.

You add a test to the existing asset reconciliation exclusion rules to stop rules from adding wifi data to the blacklist.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by the Local system and NOT when the
event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist - IP Asset Reconciliation
Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and different Identity MAC in 2 hours.
```

The updated rule tests only the events from the log sources that are not on your wifi DHCP server. To prevent wifi DHCP events from undergoing more expensive reference set and behavior analysis tests, you also moved this test to the top of the test stack.

Asset merging

Asset merging is the process where the information for one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Asset merging occurs when an asset update contains identity data that matches two different asset profiles. For example, a single update that contains a NetBIOS host name that matches one asset profile and a MAC address that matches a different asset profile might trigger an asset merge.

Some systems can cause high volumes of asset merging because they have asset data sources that inadvertently combine identity information from two different physical assets into a single asset update. Some examples of these systems include the following environments:

- Central syslog servers that act as an event proxy
- Virtual machines
- Automated installation environments
- Non-unique host names, common with assets like iPads and iPhones.
- Virtual private networks that have shared MAC addresses
- Log source extensions where the identity field is OverrideAndAlwaysSend=true

Assets that have many IP addresses, MAC addresses, or host names show deviations in asset growth and can trigger system notifications.

Related concepts
Identification of asset growth deviations

Identification of asset growth deviations

Sometimes, asset data sources produce updates that IBM QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

Asset growth deviations occur when the number of asset updates for a single device grows beyond the limit that is set by the retention threshold for a specific type of the identity information. Proper handling of asset growth deviations is critical to maintaining an accurate asset model.

At the root of every asset growth deviation is an asset data source whose data is untrustworthy for updating the asset model. When a potential asset growth deviation is identified, you must look at the source of the information to determine whether there is a reasonable explanation for the asset to accumulate large amounts of identity data. The cause of an asset growth deviation is specific to an environment.

DHCP server example of unnatural asset growth in an asset profile

Consider a virtual private network (VPN) server in a Dynamic Host Configuration Protocol (DHCP) network. The VPN server is configured to assign IP addresses to incoming VPN clients by proxying DHCP requests on behalf of the client to the network's DHCP server.

From the perspective of the DHCP server, the same MAC address repeatedly requests many IP address assignments. In the context of network operations, the VPN server is delegating the IP addresses to the clients, but the DHCP server can't distinguish when a request is made by one asset on behalf of another.

The DHCP server log, which is configured as a QRadar log source, generates a DHCP acknowledgment (DHCP ACK) event that associates the MAC address of the VPN server with the IP address that it assigned to the VPN client. When asset reconciliation occurs, the system reconciles this event by MAC address, which results in a single existing asset that grows by one IP address for every DHCP ACK event that is parsed.

Eventually, one asset profile contains every IP address that was allocated to the VPN server. This asset growth deviation is caused by asset updates that contain information about more than one asset.

Threshold settings

When an asset in the database reaches a specific number of properties, such as multiple IP addresses or MAC addresses, QRadar blocks that asset from receiving more updates.

The Asset Profiler threshold settings specify the conditions under which an asset is blocked from updates. The asset is updated normally up to the threshold value. When the system collects enough data to exceed

the threshold, the asset shows an asset growth deviation. Future updates to the asset are blocked until the growth deviation is rectified.

System notifications that indicate asset growth deviations

IBM QRadar generates system notifications to help you identify and manage the asset growth deviations in your environment.

The following system messages indicate that QRadar identified potential asset growth deviations:

- The system detected asset profiles that exceed the normal size threshold
- The asset blacklist rules have added new asset data to the asset blacklists

The system notification messages include links to reports to help you identify the assets that have growth deviations.

Asset data that changes frequently

Asset growth can be caused by large volumes of asset data that changes legitimately, such as in these situations:

- A mobile device that travels from office-to-office frequently and is assigned a new IP address whenever it logs in.
- A device that connects to a public wifi with short IP addresses leases, such as at a university campus, might collect large volumes of asset data over a semester.

Example: How configuration errors for log source extensions can cause asset growth deviations

Customized log source extensions that are improperly configured can cause asset growth deviations.

You configure a customized log source extension to provide asset updates to IBM QRadar by parsing user names from the event payload that is on a central log server. You configure the log source extension to override the event host name property so that the asset updates that are generated by the custom log source always specify the DNS host name of the central log server.

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

Troubleshooting asset profiles that exceed the normal size threshold

IBM QRadar generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

```
The system detected asset profiles that exceed the normal size threshold
```

Explanation

The payload of the notification shows a list of the top five most frequently deviating assets and why the system marked each asset as a growth deviation. As shown in the following example, the payload also shows the number of times that the asset attempted to grow beyond the asset size threshold.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer] com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
The top five most frequently deviating asset profiles between Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

When the asset data exceeds the configured threshold, QRadar blocks the asset from future updates. This intervention prevents the system from receiving more corrupted data and mitigates the performance impacts that might occur if the system attempts to reconcile incoming updates against an abnormally large asset profile.

Required user action

Use the information in the notification payload to identify the assets that are contributing to the asset growth deviation and determine what is causing the abnormal growth. The notification provides a link to a report of all assets that experienced deviating asset growth over the past 24 hours.

After you resolve the asset growth deviation in your environment, you can run the report again.

1. Click the **Log Activity** tab and click **Search** > **New Search**.
2. Select the **Deviating Asset Growth: Asset Report** saved search.
3. Use the report to identify and repair inaccurate asset data that was created during the deviation.

New asset data is added to the asset blacklists

IBM QRadar generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

```
The asset blacklist rules have added new asset data to the asset blacklists
```

Explanation

Asset exclusion rules monitor asset data for consistency and integrity. The rules track specific pieces of asset data over time to ensure that they are consistently being observed with the same subset of data within a reasonable time.

For example, if an asset update includes both a MAC address and a DNS host name, the MAC address is associated with that DNS host name for a sustained period. Subsequent asset updates that contain that MAC address also contain that same DNS host name when one is included in the asset update. If the MAC address suddenly is associated with a different DNS host name for a short period, the change is monitored. If the MAC address changes again within a short period, the MAC address is flagged as contributing to an instance of deviating or abnormal asset growth.

Required user action

Use the information in the notification payload to identify the rules that are used to monitor asset data. Click the **Asset deviations by log source** link in the notification to see the asset deviations that occurred in the last 24 hours.

If the asset data is valid, QRadar administrators can configure QRadar to resolve the problem.

- If your blacklists are populating too aggressively, you can tune the asset reconciliation exclusion rulesthat populate them.
- If you want to add the data to the asset database, you can remove the asset data from the blacklistand add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.

Asset blacklists and whitelists

IBM QRadar uses a group of asset reconciliation rules to determine if asset data is trustworthy. When asset data is questionable, QRadar uses asset blacklists and whitelists to determine whether to update the asset profiles with the asset data.

An *asset blacklist* is a collection of data that IBM QRadar considers untrustworthy. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

Your QRadar administrator can modify the asset blacklist and whitelist data to prevent future asset growth deviations.

Asset blocklists

An *asset blocklist* is a collection of data that IBM QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blocklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

Every asset update in QRadar is compared to the asset blocklists. Blocklisted asset data is applied globally for all domains. If the asset update contains identity information (MAC address, NetBIOS host name, DNS host name, or IP address) that is found on a blocklist, the incoming update is discarded and the asset database is not updated.

Table 22. Reference collection names for asset blocklist data

Type of identity data	**Reference collection name**	**Reference collection type**
IP addresses (v4)	Asset Reconciliation IPv4 Blacklist	Reference Set [Set Type: IP]
DNS host names	Asset Reconciliation DNS Blacklist	Reference Set [Set Type: ALNIC*]
NetBIOS host names	Asset Reconciliation NetBIOS Blacklist	Reference Set [Set Type: ALNIC*]
MAC Addresses	Asset Reconciliation MAC Blacklist	Reference Set [Set Type: ALNIC*]
* ALNIC is an alphanumeric type that can accommodate both host name and MAC address values.		

Your QRadar administrator can modify the blacklist entries to ensure that new asset data is handled correctly.

Asset whitelists

You can use asset whitelists to keep IBM QRadar asset data from inadvertently reappearing in the asset blacklists.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

Your QRadar administrator can modify the whitelist entries to ensure that new asset data is handled correctly.

Example of a whitelist use case

The whitelist is helpful if you have asset data that continues to show up in the blacklists when it is a valid asset update. For example, you might have a round robin DNS load balancer that is configured to rotate across a set of five IP addresses. The Asset Reconciliation Exclusion rules might determine that the multiple IP addresses associated with the same DNS host name are indicative of an asset growth deviation, and the system might add the DNS load balancer to the blacklist. To resolve this problem, you can add the DNS host name to the Asset Reconciliation DNS Whitelist.

Mass entries to the asset whitelist

An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network. Ignoring asset deviations by adding mass entries to the asset whitelist is not helpful in building an accurate asset database. Instead of adding mass whitelist entries, review the asset blacklist to determine what is contributing to the deviating asset growth and then determine how to fix it.

Types of asset whitelists

Each type of identity data is kept in a separate whitelist. The following table shows the reference collection name and type for each type of identity asset data.

Table 23. Reference collection name for asset whitelist data

Type of data	Reference collection name	Reference collection type
IP addresses	Asset Reconciliation IPv4 Whitelist	Reference Set [Set Type: IP]
DNS host names	Asset Reconciliation DNS Whitelist	Reference Set [Set Type: ALNIC*]
NetBIOS host names	Asset Reconciliation NetBIOS Whitelist	Reference Set [Set Type: ALNIC*]
MAC addresses	Asset Reconciliation MAC Whitelist	Reference Set [Set Type: ALNIC*]
* ALNIC is an alphanumeric type that can accommodate host name and MAC address values.		

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 flow data or vulnerability assessment (VA) scans configured. For flow data to populate asset profiles, bidirectional flows are required. Asset profiles can also be automatically created from identity events. For more information about VA, see the *IBM QRadar Vulnerability Assessment Guide*.

For more information about flow sources, see the *IBM QRadar Administration Guide*.

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 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 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 information about the Server Discovery option in the navigation pane, see the *IBM QRadar Administration Guide*

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

Viewing an asset profile

From the asset list on the **Assets** tab, you can select and view an asset profile. An asset profile provides information 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 24. Asset Profile page toolbar functions

Options	Description
Return to Asset List	Click this option to return to the asset list.
Display	From the list box, you can select the pane that you want to view on the Asset Profile pane. The Asset Summary and Network Interface Summary panes are always displayed.
Edit Asset	Click this option to edit the Asset Profile. See "Adding or editing an asset profile" on page 123.
View by Network	If this asset is associated with an offense, this option will allow you to view the list of networks that are associated with this asset. When you click **View By Network**, the **List of Networks** window is displayed.
View Source Summary	If this asset is the source of an offense, this option will allow you to view source summary information. When you click **View Source Summary**, the **List of Offenses** window is displayed.

Table 24. Asset Profile page toolbar functions (continued)

Options	Description
View Destination Summary	If this asset is the destination of an offense, this option will allow you to view destination summary information. When you click **View Destination Summary**, the **List of Destinations** window is displayed.
History	Click **History** to view event history information for this asset. When you click the **History** icon, the **Event Search** window is displayed, pre-populated with event search criteria: You can customize the search parameters, if required. Click **Search** to view the event history information.
Applications	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. You can customize the search parameters, if required. Click **Search** to view the application information.

Search Connections	Click **Search Connections** to search for connections. The **Connection Search** window is displayed. This option is only displayed when IBM QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM QRadar Risk Manager User Guide*.
View Topology	Click **View Topology** to further investigate the asset. The **Current Topology** window is displayed. This option is only displayed when IBM QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM QRadar Risk Manager User Guide*.
Actions	From the **Actions** list, select **Vulnerability History.** This option is only displayed when IBM QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM QRadar Risk Manager User Guide*.

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. SeeTable 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:

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

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

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

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

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

9. Click **Save**.

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 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.
4. Click **Save Criteria** .
5. Enter values for the parameters:

Parameter	**Description**
Enter the name of this search	Type the unique name that you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. This option is only displayed if you have administrative permissions.
Parameter	**Description**
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the **Other** group by default.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is on the **Assets** tab toolbar.
Set as Default	Select this check box to set this search as your default search when you access the **Assets** tab.

Share with Everyone	Select this check box to share these search requirements with all users.

What to do next

Editing a compliance benchmark

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 25. Asset Search Groups window toolbar functions

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

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
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**.
3. Select **Search** > **New Search**.
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:

Parameter	**Description**
Vulnerability ID	Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Published Date	Specifies the date on which the vulnerability details were published on the OSVDB.
Name	Specifies the name of the vulnerability.

Assets	Specifies the number of assets in your network that have this vulnerability. Click the link to view the list of assets.
Assets, including exceptions	Specifies the number of assets in your network that have vulnerability exceptions. Click the link to view the list of assets.
CVE	Specifies the CVE identifier for the vulnerability. CVE identifiers are provided by the NVDB. Click the link to obtain more information. When you click the link, the NVDB website is displayed in a new browser window.
xforce	Specifies the X-Force identifier for the vulnerability. Click the link to obtain more information. When you click the link, the IBM Internet Security Systems website is displayed in a new browser window.
OSVDB	Specifies the OSVDB identifier for the vulnerability. Click the link to obtain more information. When you click the link, the OSVDB website is displayed in a new browser window.
Plugin Details	Specifies the QRadar Vulnerability Manager ID. Click the link to view Oval Definitions, Windows Knowledge Base entries, or UNIX advisories for the vulnerability. This feature provides information on how QRadar Vulnerability Manager checks for vulnerability details during a patch scan. You can use it to identify why a vulnerability was raised on an asset or why it was not.

Parameter	**Description**

CVSS Score Base	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 123. For more information about CVSS, see http://www.first.org/cvss/ .
Impact	Displays the type of harm or damage that can be expected if this vulnerability is exploited.
CVSS Base Metrics	Displays the metrics that are used to calculate the CVSS base score, including: • Access Vector • Access complexity • Authentication • Confidentiality impact • Integrity impact • Availability impact
Description	Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.
Concern	Specifies the effects that the vulnerability can have on your network.
Solution	Follow the instructions that are provided to resolve the vulnerability.
Virtual Patching	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.
Parameter	**Description**

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

Procedure

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.

Chapter 9. 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 or flow 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 aspecified 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 or flow 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 ©

Copyright IBM Corp. 2012, 2021

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 26. Time series charts functions

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

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 aboutthe 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 thehidden 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 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.

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.

Restriction: Charts are not displayed when you view events or flows in Real Time (streaming) mode. To display charts, you must access the **Log Activity** or **Network Activity** tab and perform a grouped search that specifies a time range.

Procedure

1. Click the **Log Activity** or **Network Activity** tab.
2. To create a grouped search, follow these steps:
   a) On the toolbar, click **Search** > **New Search**.
   b) From the **Available Saved Searches**, select a search and click **Load**.
   c) Go to the Column Definition pane and if the **Group By** list box is empty, from the **Available Columns** list, select a column.
   d) Click **Search**.
3. To use a grouped search, on the toolbar, click **Quick Searches** and select a grouped search.
4. In the Charts pane, click the **Configure** icon ( ).
5. Configure the following parameters:

Parameter	Description
Value to Graph	The object type that you want to graph on the Y axis of the chart. Options include all normalized and custom event or flow parameters that are included in your search parameters.

Display Top	The number of objects that you want to view in the chart. The default is 10. If you include more than 10 items in your chart, your data might be illegible.
Chart Type	If your bar, pie, or table chart is based on saved search criteria with a time range of more than 1 hour, you must click **Update Details** to update the chart and populate the event details.
Capture Time Series Data	Enables time series data capture. When you select this check box, the chart begins accumulating data for time series charts. By default, this option is disabled. This option is available only on Time Series charts.
Time Range	The time range that you want to view.

Parameter	Description
	This option is only available on Time Series charts.

6. If you selected the **Time Series** chart option and enabled the **Capture Time Series Data** option, in the Charts pane, click **Save** .
7. To view the list of events or flows if your time range is greater than 1 hour, click **Update Details**.

Chapter 10. Event and flow searches

You can perform searches on the **Log Activity**, **Network Activity**, and **Offenses** tabs.

Use search and index options in IBM QRadar that improve search performance and return quicker results. To find specific criteria, advanced searches use AQL search strings.

You can specify filter criteria to search for events, flows, and offenses. After you perform a search, you can save the search criteria and the search results.

If your QRadar administrator configured resource restrictions to set time or data limitations on event and flow searches, the resource restriction icon ( ) appears next to the search criteria.

Related concepts Quick filter search options
Search event and flow payloads by typing a text search string that uses simple words or phrases.

Creating a customized search

You can search for data that match your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

About this task

The duration of your search varies depending on the size of your database.

You can add new search options to filter through search results to find a specific event or flow that you are looking for.

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

Table 27. Search options

Options	Description
Group	Select an event search group or flow search group to view in the **Available Saved Searches** list.
Type Saved Search or Select from List	Type the name of a saved search or a keyword to filter the **Available Saved Searches** list.
Available Saved Searches	This list displays all available searches, unless you 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.
Search	The **Search** icon is available in multiple panes on the search page. You can click Search when you are finished configuring the search and want to view the results.

Include in my Quick Searches	Select this check box to include this search in your **Quick Search** menu.

© Copyright IBM Corp. 2012, 2021

Table 27. Search options (continued)

Options	**Description**
Include in my Dashboard	Select this check box to include the data from your saved search on the **Dashboard** tab. For more information about the **Dashboard** tab, see Dashboard management. **Note:** This parameter is only displayed if the search is grouped.
Set as Default	Select this check box to set this search as your default search.
Share with Everyone	Select this check box to share this search with all other users.
Real Time (streaming)	Displays results in streaming mode. **Note:** When Real Time (streaming) is enabled, you are unable to group your search results. If you select any grouping option in the Column Definition pane, an error message opens.
Last Interval (auto refresh)	The **Log Activity** and **Network Activity** tabs are refreshed at one-minute intervals to display the most recent information.
Recent	After you select this option, you must select a time range option from the list. **Note:** The results from the last minute might not be available. Select the <*Specific Interval*> option if you want to see all results.
Specific Interval	After you select this option, you must select the date and time range from the **Start Time** and **End Time** calendars.

Data Accumulation	Displayed when you load a saved search. If no data is accumulating for this saved search, the following information message is displayed: Data is not being accumulated for this search. If data is accumulating for this saved search, the following options are displayed: When you click or hover your mouse over the column link, a list of the columns that are accumulating data opens. Use the **Enable Unique Counts/Disable Unique Counts** link to display unique event and flow counts instead of average counts over time. After you click the **Enable Unique Counts** link, a dialog box opens and indicates which saved searches and reports share the accumulated data.
Current Filters	Displays the filters that are applied to this search.
Save results when the search is complete	Saves the search results.

Table 27. Search options (continued)	
Options	**Description**
Display	Species a predefined column that is set to display in the search results.
Name	The name of your custom column layout.
Save Column Layout	Saves a custom column layout that you modified.
Delete Column Layout	Deletes a saved custom column layout.
Type Column or Select from List	Filter the columns that are listed in the Available Columns list. For example, type Device to display a list of columns that include Device in the column name.
Available Columns	Columns that are currently in use for this saved search are highlighted and displayed in the **Columns** list.
Add and remove column arrows (top set)	Use the top set of arrows to customize the **Group By** list. • To add a column, select one or more columnsfrom the **Available Columns** list and click the right arrow. • To remove a column, select one or more columnsfrom the **Group By** list and click the left arrow.
Add and remove column arrows (bottom set)	Use the bottom set of arrows to customize the **Columns** list. • To add a column, select one or more columnsfrom the **Available Columns** list and click the right arrow. • To remove a column, select one or more columnsfrom the **Columns** list and click the left arrow.

Group By	Specifies the columns on which the saved search groups the results. • To move a column up the priority list, select acolumn and click the up arrow. You can also drag the column up the list. • To move a column down the priority list, select acolumn and click the down arrow. You can also drag the column down the list. The priority list specifies in which order the results are grouped. The search results are grouped by the first column in the **Group By** list and then grouped by the next column on the list. **Note:** The search may not return the correct results if you include domains in the **Group By** list.

Table 27. Search options (continued)

Options	**Description**
Columns	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: • To move a column up the priority list, select acolumn and click the up arrow. You can also drag the column up the list. • To move a column down the priority list, select acolumn and click the down arrow. You can also drag the column down the list. If the column type is numeric or time-based and an entry is in the **Group By** list, then the column includes a list. Use the list to choose how you want to group the column. If the column type is group, the column includes a list to choose how many levels that you want to include for the group.
Move columns between the Group By list and the Columns list	Move columns between the **Group By** list and the **Columns** list by selecting a column in one list and dragging it to the other.
Order By	From the first list, select the column by which you want to sort the search results. Then, from the second list, select the order that you want to display for the search results.

Results Limit	Specifies the number of rows that 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 thesaved search and re-applied when search is loaded. • When you are sorting a column in the searchresult that has a row limit, sorting is done within the limited rows, which are shown in the data grid. • For a grouped by search where time series chartis turned on, the row limit applies only to the data grid. The **Top N** list in the time series chart controls how many time series are drawn in the chart.

Procedure

1. Choose a search option:
   - To search events, click the **Log Activity** tab.
   - To search flows, click the **Network Activity** tab.
2. From the **Search** list, select **New Search**.
3. Select a previously saved search.
4. To create a search, in the Time Range pane, select the options for the time range that you want tocapture for this search.

   Note: The time range that you select might impact performance, when the time range is large.
5. Enable unique counts in the **Data Accumulation** pane.

   Note: Enabling unique counts on accumulated data, which is shared with many other saved searches and reports might decrease system performance.
6. In the Search Parameters pane, define your search criteria.
   a) From the first list, select a parameter that you want to search for.
   b) From the second list, select the modifier that you want to use for the search.

   Note:

   To search for an event or flow whose custom property does not have a value, use the "is N/A" operator. To search for an event or flow whose custom property has a value, use the "is not N/A" operator.

   c) From 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 are adding to the search criteria.
7. 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 that you want to use to view the results:
   a) From the **Display** list, 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.

d) In the **Results Limit** field, type the number of rows that you want the search to return.

Tip: If you configure a log source that belongs to multiple log source groups but has only one event that matches your search criteria, the search generates results for each log source group (including the parent group) that the event belongs to. This is expected behavior.

9. Click **Filter**.

Creating a custom column layout

Create a custom column layout by adding or removing columns in an existing layout.

Procedure

1. On the **Log Activity** or the **Network Activity** tab, click **Search** > **Edit Search**.
2. In the **Column Definition** pane, select an existing column layout in the **Display** list.

   When you modify the layout, the name in the **Display** list is automatically changed to *Custom*.
3. Modify your search grouping.
   a) To add a column to your search group, select a column from the **Available Columns** list and click the right arrow to move the column to the **Group By** list.
   b) To move a column from the **Columns** list to your search group, select a column from the **Columns** list and drag it to the **Group By** list.
   c) To remove a column from your search group, select the column from the **Group By** list and click the left arrow.
   d) To change the order of your column groupings, use the up and down arrows or drag the columnsinto place.
4. Modify your column layout.
   a) To add a column to your custom layout, select a column from the **Available Columns** list and click the right arrow to move the column to the **Columns** list.
   b) To move a column from the **Group By** list to your custom layout, select a column from the **Group By** list and drag it to the **Columns** list.
   c) To remove a column from your custom layout, select the column from the **Columns** list and click the left arrow.
   d) To change the order of your columns, use the up and down arrows or drag the columns into place.
5. In the **Name** field, enter the name of your custom column layout.
6. Click **Save Column Layout**.

Deleting a custom column layout

You can delete an existing user-created column layout.

Procedure

1. On the **Log Activity** or the **Network Activity** tab, click **Search** > **Edit Search**.
2. In the **Column Definition** pane, select an existing user-created column layout in the **Display** list.
3. Click **Delete Column Layout**.

Querying with dynamic search

Use the dynamic search API to search for data that involves aggregated functions, such as **COUNT**, **SUM**, **MAX**, and **AVG**. For example, you can count the number of asset IDs per asset hostname by using the **COUNT_PER** function.

About this task

You can build your query on the following data sources:

- Assets
- Offenses
- Vulninstances

You can add a field without a function as a simple field, or you can add a field with a function as a complex field to build columns. You can also add conditions to filter your data.

Procedure

1. Click the **Admin** tab.
2. In the **Dynamic Search** section, click **Dynamic Search**.
3. Select a **Data Source**.
4. Complete the **Available Columns** and **Available Filters** sections.
5. To add a name, description, range of the search, retention period, or search type to your query, enableone or more **Extra Search Properties**.
6. To copy your JSON script, click **Generate JSON**.

   Your results appear in the **JSON generated by your query** section. Click **Copy to Clipboard** to copy your JSON script.
7. To reset your selections, click **Reset**.
8. Click **Run Query**.

Results

The results of your query are listed in plain text or link format. For example, if you chose to query the **ASSET_ID** field, you can click the results to view the **Asset Summary** window for each asset ID.

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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Perform a search.
3. Click **Save Criteria**.
4. Enter values for the parameters:

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

5. Click **OK**.

Scheduled search

Use the Scheduled search option to schedule a search and view the results.

You can schedule a search that runs at a specific time of day or night. If you schedule a search to run in the night, you can investigate in the morning. Unlike reports, you have the option of grouping the search results and investigating further. You can search on number of failed logins in your network group. If the result is typically 10 and the result of the search is 100, you can group the search results for easier investigating. To see which user has the most failed logins, you can group by user name. You can continue to investigate further.

You can schedule a search on events or flows from the **Reports** tab. You must select a previously saved set of search criteria for scheduling.

1. Create a report

   Specify the following information in the **Report Wizard** window:

   - The chart type is Events/Logs or Flows.
   - The report is based on a saved search.

     Note: QRadar does not support reports based on AQL searches that contain subselect statements.
   - Generate an offense.

     You can choose the **create an individual offense** option or the **add result to an existing offense** option.

     You can also generate a manual search.
2. View search results

You can view the results of your scheduled search from the **Offenses** tab.

- Scheduled search offenses are identified by the **Offense Type** column.

  If you create an individual offense, an offense is generated each time that the report is run. If you add the saved search result to an existing offense, an offense is created the first time that the report runs. Subsequent report runs append to this offense. If no results are returned, the system does not append or create an offense.
- To view the most recent search result in the **Offense Summary** window, double-click a scheduled search offense in the offense list. To view the list of all scheduled search runs, click **Search Results** in the **Last 5 Search Results** pane.

You can assign a Scheduled search offense to a user.

Related tasks

Creating a customized search

You can search for data that match your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

Assigning offenses to users

By default, all new offenses are unassigned. You can assign an offense to an IBM QRadar user for investigation.

Quick filter search options

Search event and flow payloads by typing a text search string that uses simple words or phrases.

Quick filter is one of the fastest methods that you use to search for event or flow payloads for specific data. For example, you can use quick filter to find these types of information:

- Every firewall device that is assigned to a specific address range in the past week
- A series of PDF files that were sent by a Gmail account in the past five days
- All records in a two-month period that exactly match a hyphenated user name
- A list of website addresses that end in .ca

You can filter your searches from these locations:

Log Activity toolbar and Network Activity toolbars
Select **Quick Filter** from the list box on the **Search** toolbar to type a text search string. Click the **Quick Filter** icon to apply your **Quick Filter** to the list of events or flows.

Add Filter Dialog box
Click the **Add Filter** icon on the **Log Activity** or **Network Activity** tab.

Select **Quick Filter** as your filter parameter and type a text search string.

Flow search pages
Add a quick filter to your list of filters.

Note: Quick Filter searches that use a time frame outside of the Payload Index Retention setting can trigger slow and resource-intensive system responses. For example, if the payload index retention is set for 1 day, and you use a time frame for the last 30 hours in the search.

When you view **flows** in real-time (streaming) or last interval mode, you can type only simple words or phrases in the **Quick Filter** field. When you view **events** or **flows** in a time-range, follow these syntax guidelines:

Table 28. Quick filter syntax guidelines

Description	Example
Include any plain text that you expect to find in the payload.	Firewall
Search for exact phrases by including multiple terms in double quotation marks.	"Firewall deny"
Include single and multiple character wildcards. The search term cannot start with a wildcard.	F?rewall or F??ew*
Group terms with logical expressions, such as AND, OR, and NOT. To be recognized as logical expressions and not as search terms, the syntax and operators must be uppercase.	(%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, no results are returned.	(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)

Precede the following characters by a backslash to indicate that the character is part of your search term: + - && || ! () {} [] ^ " ~ * ? : \.	"%PIX\-5\-304001"

Limitations

Quick filter searches operate on raw event or flow log data and don't distinguish between the fields. For example, quick filter searches return matches for both source IP address and destination IP address, unless you include terms that can narrow the results.

Search terms are matched in sequence from the first character in the payload word or phrase. The search term user matches user_1 and user_2, but does not match the following phrases: ruser, myuser, or anyuser.

Quick filter searches use the English locale. *Locale* is a setting that identifies language or geography and determines formatting conventions such as collation, case conversion, character classification, the language of messages, date and time representation, and numeric representation.

The locale is set by your operating system. You can configure QRadar to override the operating system locale setting. For example, you can set the locale to **English** and the QRadar Console can be set to **Italiano (Italian)**.

If you use Unicode characters in your quick filter search query, unexpected search results might be returned.

If you choose a locale that is not English, you can use the Advanced search option in QRadar for searching event and payload data.

How does Quick Filter search and payload tokens work?

Text that is in the payload is split into words, phrases, symbols, or other elements. These tokens are delimited by space and punctuation. The tokens don't always match user-specified search terms, which cause some search terms not to be found when they don't match the generated token. The delimiter characters are discarded but exceptions exist such as the following exceptions:

- Periods that are not followed by white space are included as part of the token.

  For example, 192.0.2.0:56 is tokenized as host token 192.0.2.0 and port token 56.
- Words are split at hyphens, unless the word contains a number, in which case, the token is not split andthe numbers and hyphens are retained as one token.
- Internet domain names and email addresses are preserved as a single token.

  192.0.2.0/home/www is tokenized as one token and the URL is not separated.

  192.0.2.7:/calling1/www2/scp4/path5/fff is tokenized as host 192.0.2.7 and the remainder is one token /calling1/www2/scp4/path5/fff

File names and URL names that contain more than one underscore are split before a period (.).

Example of multiple underscores in a file name:

If you use hurricane_katrina_ladm118.jpg as a search term, it is split into the following tokens:

- hurricane
- katrina_ladm118.jpg

Search the payload for the full search term by placing double quotation marks around the search term:

"hurricane_katrina_ladm118.jpg"

Example of multiple underscores in a relative file path:

The thumb.ladm1180830/thumb.ladm11808301806.hurricane_katrina_ladm118.jpg is split into the following tokens:

- thumb.ladm1180830/thumb.ladm11808301806.hurricane
- katrina_ladm118.jpg

To search for hurricane_katrina_ladm118.jpg, which consists of one partial and one full token, place an asterisk in front of the query term, *hurricane_katrina_ladm118.jpg

Related concepts Event and flow searches

You can perform searches on the **Log Activity**, **Network Activity**, and **Offenses** tabs.

Advanced search options

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

Note: When you type an AQL query, use single quotation marks for a string comparison, and use double quotation marks for a property value comparison.

The **Advanced Search** field has auto completion and syntax highlighting.

Use auto completion and syntax highlighting to help create queries. For information about supported web browsers, see "Supported web browsers " on page 6

Note: If you use a quick filter on the **Log Activity** tab, you must refresh your browser window before you run an advanced search.

Accessing Advanced Search

Access the **Advanced Search** option from the **Search** toolbar that is on the **Network Activity** and **Log Activity** tabs to type an AQL query.

Select **Advanced Search** from the list box on the **Search** toolbar.

Expand the **Advanced Search** field by following these steps:

1. Drag the expand icon that is at the right of the field.
2. Press Shift + Enter to go to the next line.
3. Press Enter.

You can right-click any value in the search result and filter on that value.

Double-click any row in the search result to see more detail.

All searches, including AQL searches, are included in the audit log.

AQL search string examples

The following table provides examples of AQL search strings.

Table 29. Examples of AQL search strings	
Description	**Example**
Select default columns from events. Select default columns from flows.	SELECT * FROM events SELECT * FROM flows
Select specific columns.	SELECT sourceip, destinationip FROM events
Select specific columns and order the results.	SELECT sourceip, destinationip FROM events ORDER BY destinationip
Run an aggregated search query.	SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip
Run a function call in a SELECT clause.	SELECT CATEGORYNAME(category) AS namedCategory FROM events
Table 29. Examples of AQL search strings (continued)	
Description	**Example**
Filter the search results by using a WHERE clause.	SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1
Search for events that triggered a specific rule, which is based on the rule name or partial text in the rule name.	SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'
Reference field names that contain special characters, such as arithmetic characters or spaces, by enclosing the field name in double quotation marks.	SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'

The following table provides examples of AQL search strings for X-Force.

Table 30. Examples of AQL search strings for X-Force	
Description	**Example**
Check an IP address against an X-Force category with a confidence value.	select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)> 3
Search for X-Force URL categories associated with a URL.	select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL

Retrieve X-Force IP categories that are associated with an IP.	select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL

For more information about functions, search fields and operators, see the *Ariel Query Language guide*.

AQL search string examples

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Note: When you build an AQL query, if you copy text that contains single quotation marks from any document and paste the text into IBM QRadar, your query will not parse. As a workaround, you can paste the text into QRadar and retype the single quotation marks, or you can copy and paste the text from the IBM Knowledge Center.

Reporting account usage

Different user communities can have different threat and usage indicators.

Use reference data to report on several user properties, for example, department, location, or manager. You can use external reference data.

The following query returns metadata information about the user from their login events.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Insight across multiple account identifiers

In this example, individual users have multiple accounts across the network. The organization requires a single view of a users activity.

Use reference data to map local user IDs to a global ID.

The following query returns the user accounts that are used by a global ID on events that are flagged as suspicious.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

The following query shows the activities that are completed by a global ID.

```
SELECT
QIDNAME(qid) as 'Event name', starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identify suspicious long-term beaconing

Many threats use command and control to communicate periodically over days, weeks, and months.

Advanced searches can identify connection patterns over time. For example, you can query consistent, short, low volume, number of connections per day/week/month between IP addresses, or an IP address and geographical location.

The following query detects potential instances of hourly beaconing.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'HH')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING "different hours" > 20
AND "total flows" < 25
LAST 24 hours
```

Tip: You can modify this query to work on proxy logs and other event types.

The following query detects potential instances of daily beaconing.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING "different days" > 4
AND "total flows" < 14
LAST 7 days
```

The following query detects daily beaconing between a source IP and a destination IP. The beaconing times are not at the same time each day. The time lapse between beacons is short.

```
SELECT sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and "total flows" < 10
LAST 7 days
```

The following query detects daily beaconing to a domain by using proxy log events. The beaconing times are not at the same time each day. The time lapse between beacons is short.

```
SELECT sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
```

```
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and "total events" < 10
LAST 7 days
```

The **url_domain** property is a custom property from proxy logs.

External threat intelligence

Usage and security data that is correlated with external threat intelligence data can provide important threat indicators.

Advanced searches can cross-reference external threat intelligence indicators with other security events and usage data.

This query shows how you can profile external threat data over many days, weeks, or months to identify and prioritize the risk level of assets and accounts.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Asset intelligence and configuration

Threat and usage indicators vary by asset type, operating system, vulnerability posture, server type, classification, and other parameters.

In this query, advanced searches and the asset model provide operational insight into a location.

The **Assetproperty** function retrieves property values from assets, which enables you to include asset data in the results.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

The following query shows how you can use advanced searches and user identity tracking in the asset model.

The **AssetUser** function retrieves the user name from the asset database.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY "Total Flows" DESC
LAST 3 HOURS
```

Network LOOKUP function

You can use the **Network LOOKUP** function to retrieve the network name that is associated with an IP address.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Rule LOOKUP function

You can use the **Rule LOOKUP** function to retrieve the name of a rule by its ID.

```
SELECT RULENAME(123) FROM events
```

The following query returns events that triggered a specific rule name.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Full TEXT SEARCH

You can use the TEXT SEARCH operator to do full text searches by using the **Advanced search** option.

In this example, there are a number of events that contain the word "firewall" in the payload. You can search for these events by using the **Quick filter** option and the **Advanced search** option on the **Log Activity** tab.

- To use the **Quick filter** option, type the following text in the **Quick filter** box: 'firewall'
- To use the **Advanced search** option, type the following query in the **Advanced search** box:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

Custom property

You can access custom properties for events and flows when you use the **Advanced search** option.

The following query uses the custom property "MyWebsiteUrl" to sort events by a particular web URL:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Related tasks

Creating a custom property

Create a custom property to extract data that IBM QRadar does not typically show from the event or flow payloads. Custom properties must be enabled, and extraction-based custom properties must be parsed, before you can use them in rules, searches, reports, or for offense indexing.

Converting a saved search to an AQL string

Convert a saved search to an AQL string and modify it to create your own searches to quickly find the data you want. Now you can create searches faster than by typing the search criteria. You can also save the search for future use.

Procedure

1. Click the **Log Activity** or **Network Activity** tab.

2. From the **Search** list, select **New Search** or **Edit Search**.
3. Select a previously saved search.
4. Click **Show AQL**.
5. From the **AQL** window, click **Copy to Clipboard**.
6. In the **Search Mode** section, click **Advanced Search**.
7. Paste the AQL string text into the **Advanced Search** text box.
8. Modify the string to include the data you want to find.
9. Click **Search** to display the results.

What to do next

Save the search criteria so that the search appears in your list of saved searches and can be reused.

Related concepts

"Advanced search options" on page 149
Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

"AQL search string examples" on page 150
Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Related tasks

"Creating a customized search" on page 139
You can search for data that match your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

"Saving search criteria" on page 145
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.

Offense searches

You can search offenses by using specific criteria to display offenses that match the search criteria in a results list.

You can create a new search or load a previously saved set of search criteria.

Searching offenses on the My Offenses and All Offenses pages

On the **My Offenses** and **All Offenses** pages of the **Offense** tab, you can search for offenses that match your criteria.

About this task

The following table describes the search options that you can use to search offense data on the **My Offenses** and **All Offenses** pages.

For information about categories, see the *IBM QRadar Administration Guide*.

Table 31. My Offenses and All Offenses page search options

Options	Description
Group	This list box allows you to select an offense Search Group to view in the **Available Saved Searches** list.
Type Saved Search or Select from List	This field allows you to type the name of a saved search or a keyword to filter the **Available Saved Searches** list.
Available Saved Searches	This list displays all available searches, unless you apply a filter to the list using the Group or Type Saved Search or Select from **List** options. You can select a saved search on this list to display or edit.
All Offenses	This option allows you to search all offenses regardless of time range.
Recent	This option allows you to select a pre-defined time range you want to filter for. After you select this option, you must select a time range option from the list box.
Specific Interval	This option allows you to configure a custom time range for your search. After you select this option, you must select one of the following options. • **Start Date between** - Select this check box to search offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search. • **Last Event/Flow between** - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Offense Id	In this field, you can type the Offense ID you want to search for.
Description	In this field, you can type the description that you want to search for.

Table 31. My Offenses and All Offenses page search options (continued)

Options	Description

Assigned to user	From this list box, you can select the user name that you want to search for.
Direction	From this list box, you can select the offense direction that you want to search for. Options include: • Local to Local • Local to Remote • Remote to Local • Remote to Remote • Local to Remote or Local • Remote to Remote or Local
Source IP	In this field, you can type the source IPv4 or IPv6 address or CIDR range you want to search for.
Destination IP	In this field, you can type the destination IPv4 or IPv6 address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude and then select to display only offenses with a magnitude that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Severity	From this list box, you can specify a severity and then select to display only offenses with a severity that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Credibility	From this list box, you can specify a credibility and then select to display only offenses with a credibility that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Relevance	From this list box, you can specify a relevance and then select to display only offenses with a relevance that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Contains Username	In this field, you can type a regular expression (regex) statement to search for offenses containing a specific user name. 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.
Source Network	From this list box, you can select the source network that you want to search for.
Destination Network	From this list box, you can select the destination network that you want to search for.

High Level Category	From this list box, you can select the high-level category that you want to search for. .

Table 31. My Offenses and All Offenses page search options (continued)

Options	Description
Low Level Category	From this list box, you can select the low-level category that you want to search for.
Exclude	The options in this pane allow you to exclude offenses from the search results. The options include: • Active Offenses • Hidden Offenses • Closed Offenses • Inactive offenses • Protected Offense
Close by User	This parameter is only displayed when the **Closed Offenses** check box is cleared in the Exclude pane. From this list box, you can select the user name that you want to search closed offenses for or select Any to display all closed offenses.
Reason For Closing	This parameter is only displayed when the **Closed Offenses** check box is cleared in the Exclude pane. From this list box, you can select a reason that you want to search closed offenses for or select **Any** to display all closed offenses.
Events	From this list box, you can specify an event count and then select to display only offenses with an event count that is equal to, less than, or greater than the configured value.
Flows	From this list box, you can specify a flow count and then select to display only offenses with a flow count that is equal to, less than, or greater than the configured value.
Total Events/Flows	From this list box, you can specify a total event and flow count and then select to display only offenses with a total event and flow count that is equal to, less than, or greater than the configured value.

Destinations	From this list box, you can specify a destination IP address count and then select to display only offenses with a destination IP address count that is equal to, less than, or greater than the configured value.
Log Source Group	From this list box, you can select a log source group that contains the log source you want to search for. The **Log Source** list box displays all log sources that are assigned to the selected log source group.

Table 31. My Offenses and All Offenses page search options (continued)

Options	**Description**
Log Source	From this list box, you can select the log source that you want to search for.
Rule Group	From this list box, you can select a rule group that contains the contributing rule that you want to search for. The **Rule** list box displays all rules that are assigned to the selected rule group.
Rule	From this list box, you can select the contributing rule that you want to search for.
Offense Type	From this list box, you can select an offense type that you want to search for. For more information about the options in the **Offense Type** list box, see Table 2.

The following table describes the options available in the **Offense Type** list box:

Table 32. Offense type options

Offense types	**Description**
Any	This option searches all offense sources.
Source IP	To search for offenses with a specific source IP address, you can select this option, and then type the source IP address that you want to search for.
Destination IP	To search for offenses with a specific destination IP address, you can select this option, and then type the destination IP address that you want to search for.

Event Name	To search for offenses with a specific event name, you can click the **Browse** icon to open the Event Browser and select the event name (QID) you want to search for. You can search for a particular QID using one of the following options: • To search for a QID by category, select the**Browse by Category** check box and select the high- or low-level category from the list boxes. • To search for a QID by log source type, selectthe **Browse by Log Source** Type check box and select a log source type from the **Log Source Type** list box. • To search for a QID by log source type, selectthe **Browse by Log Source Type** check box and select a log source type from the **Log Source Type** list box. • To search for a QID by name, select the **QID Search** check box and type a name in the **QID/ Name** field.

Table 32. Offense type options (continued)

Offense types	**Description**
Username	To search for offenses with a specific user name, you can select this option, and then type the user name that you want to search for.
Source MAC Address	To search for offenses with a specific source MAC address, you can select this option, and then type the source MAC address that you want to search for.
Destination MAC Address	To search for offenses with a specific destination MAC address, you can select this option, and then type the destination MAC address that you want to search for.
Log Source	From the **Log Source Group** list box, you can select the log source group that contains the log source you want to search for. The **Log Source** list box displays all log sources that are assigned to the selected log source group. From the **Log Source** list box, select the log source that you want to search for.
Host Name	To search for offenses with a specific host name, you can select this option, and then type the host name that you want to search for.

Source Port	To search for offenses with a specific source port, you can select this option, and then type the source port that you want to search for.
Destination Port	To search for offenses with a specific destination port, you can select this option, and then type the destination port that you want to search for.
Source IPv6	This offense type exists for backward compatibility and appears only if a Source IPv6 index was created in version 7.3.0 or earlier. To search for an older offense with a source IPv6 address, select this option and type the source IPv6 address. To search for IPv4 and IPv6 offenses that were created in version 7.3.1 or later, select the Source IP option instead.
Destination IPv6	This offense type exists for backward compatibility and appears only if a Destination IPv6 index was created in version 7.3.0 or earlier. To search for an older offense with a destination IPv6 address, select this option and type the destination IPv6 address. To search for IPv4 and IPv6 offenses that were created in version 7.3.1 or later, select the Destination IP option instead.

Table 32. Offense type options (continued)

Offense types	**Description**
Source ASN	To search for offenses with a specific Source ASN, you can select the source ASN from the **Source ASN** list box.
Destination ASN	To search for offenses with a specific destination ASN, you can select the destination ASN from the **Destination ASN** list box.
Rule	To search for offenses that are associated with a specific rule, you can select the rule group that contains the rule you want to search from the **Rule Group** list box. The **Rule Group** list box displays all rules that are assigned to the selected rule group. From the **Rule** list box, you select the rule that you want to search for.
App ID	To search for offenses with an application ID, you can select the application ID from the **App ID** list box.

Procedure

1. Click the **Offenses** tab.

2. From the **Search** list box, select **New Search**.
3. Choose one of the following options:
   - To load a previously saved search, go to Step 4.
   - To create a new search, go to Step 7.
4. Select a previously saved search using one of the following options:
   - 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.
5. Click **Load**.
6. Optional. Select the **Set as Default** check box in the Edit Search pane to set this search as your default search. If you set this search as your default search, the search automatically performs and displays results each time you access the **Offenses** tab.
7. On the Time Range pane, select an option for the time range you want to capture for this search. SeeTable 1.
8. On the Search Parameters pane, define your specific search criteria. See Table 1.
9. On the Offense Source pane, specify the offense type and offense source you want to search:
   a) From the list box, select the offense type that you want to search for.
   b) Type your search parameters. See Table 2.
10. In the Column Definition pane, define the order in which you want to sort the results:
    a) From the first list box, select the column by which you want to sort the search results.
    b) From the second list box, select the order that you want to display for the search results. Optionsinclude Descending and Ascending.
11. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Source IP page

This topic provides the procedure for how to search offenses on the **By Source IP** page of the **Offense** tab.

About this task

The following table describes the search options that you can use to search offense data on the **By Source IP** page:

Table 33. By Source IP page search options

Options	Description
All Offenses	You can select this option to search all source IP addresses regardless of time range.
Recent	You can select this option and, from this list box, select the time range that you want to search for.

Specific Interval	To specify an interval to search for, you can select the Specific Interval option and then select one of the following options: • **Start Date between** - Select this check box to search source IP addresses associated with offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search for. • **Last Event/Flow between** - Select this check box to search source IP addresses associated with offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search for.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Source IP	In this field, you can type the source IPv4 or IPv6 address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value. The range is 0 - 10.
VA Risk	From this list box, you can specify a VA risk and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Events/Flows	From this list box, you can specify an event or flow count and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.

Table 33. By Source IP page search options (continued)

Options	**Description**
Exclude	You can select the check boxes for the offenses you want to exclude from the search results. The options include: • **Active Offenses** • **Hidden Offenses** • **Closed Offenses** • **Inactive offenses** • **Protected Offense**

Procedure

1. Click the **Offenses** tab.
2. Click **By Source IP**.
3. From the **Search** list box, select **New Search**.
4. On the Time Range pane, select an option for the time range you want to capture for this search. SeeTable 1.
5. On the Search Parameters pane, define your specific search criteria. See Table 1.
6. On the Column Definition pane, define the order in which you want to sort the results:
   a) From the first list box, select the column by which you want to sort the search results.
   b) From the second list box, select the order that you want to display for the search results. Optionsinclude **Descending** and **Ascending**.
7. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Destination IP page

On the **By Destination IP** page of the **Offense** tab, you can search offenses that are grouped by the destination IP address.

About this task

The following table describes the search options that you can use to search offenses on the **By Destination IP** page:

Table 34. By Destination IP page search options	
Options	**Description**
All Offenses	You can select this option to search all destination IP addresses regardless of time range.
Recent	You can select this option and, From this list box, select the time range that you want to search for.
Table 34. By Destination IP page search options (continued)	
Options	**Description**
Specific Interval	To specify a particular interval to search for, you can select the **Specific Interval** option, and then select one of the following options: • To specify a particular interval to search for, youcan select the **Specific Interval** option, and then select one of the following options: • **Last Event/Flow between** - Select this check box to search destination IP addresses associated with offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search

Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Destination IP	You can type the destination IPv4 or IPv6 address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value. The range is 0 - 10.
Events/Flows	From this list box, you can specify an event or flow count magnitude, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **By Destination IP**.
3. From the **Search** list box, select **New Search**.
4. On the Time Range pane, select an option for the time range you want to capture for this search. SeeTable 1.
5. On the Search Parameters pane, define your specific search criteria. See Table 1.
6. On the Column Definition pane, define the order in which you want to sort the results:
   a) From the first list box, select the column by which you want to sort the search results.
   b) From the second list box, select the order in which you want to display the search results. Optionsinclude **Descending** and **Ascending**.
7. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Networks page

On the **By Network page** of the **Offense** tab, you can search offenses that are grouped by the associated networks.

About this task

The following table describes the search options that you can use to search offense data on the **By Networks** page:

Table 35. Search options for search offense data on the By Networks page

Option	Description

Network	From this list box, you can select the network that you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value.
Event/Flows	From this list box, you can specify an event or flow count, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

1. Click the **Offenses** tab.
2. Click **By Networks**.
3. From the **Search** list box, select **New Search**.
4. On the Search Parameters pane, define your specific search criteria. See Table 1.
5. On the Column Definition pane, define the order in which you want to sort the results:
   a) From the first list box, select the column by which you want to sort the search results.
   b) From the second list box, select the order in which you want to display the search results. Optionsinclude **Descending** and **Ascending**.
6. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Saving search criteria on the Offenses tab

On the **Offenses** tab, you can save configured search criteria so that you can reuse the criteria for future searches. Saved search criteria does not expire.

Procedure

1. Procedure
2. Perform a search. See Offense searches.
3. Click **Save Criteria**.
4. Enter values for the following parameters:

Option	**Description**
Parameter	Description
Search Name	Type a name you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. See Managing search groups.

Timespan options:	Choose one of the following options: • **All Offenses** - Select this option to search all offenses regardless of time range. • **Recent** - Select the option and, from this list box, select the time range that you want to search for. • **Specific Interval** - To specify a particular interval to search for, select the **Specific Interval** option, and then select one of the following options: Start Date between - Select this check box to search offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search for. Last Event/Flow between - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.Last Event between - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.
Set as Default	Select this check box to set this search as your default search.

5. Click **OK**.

Searching for offenses that are indexed on a custom property

Define search criteria to filter the offense list and make it easier to see which offenses you need to investigate. You can use the offense type in your search criteria to find all offenses that are based on a custom property. You can filter the query results to show offenses that have a specific custom property capture result.

Before you begin

The custom property must be used as a rule index. For more information, see "Offense indexing" on page 28.

Procedure

1. Click the **Offenses** tab.
2. From the **Search** list, select **New Search**.
3. On the **Offense Source** pane, select the custom property in the **Offense Type** list.

   The **Offense Type** list shows only normalized fields and custom properties that are used as rule indexes. You cannot use **Offense Source** to search DateTime properties.
4. Optional: To search for offenses that have a specific value in the custom property capture result, type the value that you want to search for in the filter box.
5. Configure other search parameters to satisfy your search requirements.
6. Click **Search**.

Results

All offenses that meet the search criteria are shown in the offense list. When you view the offense summary, the custom property that you searched on is shown in the **Offense Type** field. The custom property capture result is shown in the **Custom Property Value** field in the **Offense Source Summary** pane.

Finding IOCs quickly with lazy search

You use the IBM QRadar *lazy search* to search for an indicator of compromise (IOC), such as unusual outbound network traffic or anomalies in privileged user account activity.

Before you begin

Lazy search returns the first 1000 events that are related to the search criterion. For example, if you need to search for a particular MD5 as part of a malware outbreak investigation, you do not need to review every related event. Do a *lazy search* to quickly return a limited result set.

To take advantage of the *lazy search*, you must have the Admin security profile, or a non-administrator security profile that is configured in the following way:

- Permission precedence set to **No Restrictions**.
- Access to all networks and log sources.

Lazy search cannot be used by users with non-administrator security profiles on networks where domains are configured.

Procedure

1. To do a lazy search for quick filters, do these steps:
   a) On the **Log Activity** tab, in the **Quick Filter** field, enter a value.
   b) From the **View** list, select a time range.
2. To do a lazy search for basic searches, do these steps:
   a) On the Log Activity tab, click **Search** > **New Search**.
   b) Select a **Recent** time range or set a **Specific Interval**.
   c) Ensure that **Order by** field value is set to Start Time and the **Results Limit** field value is 1000 or less. Aggregated columns must not be included in the search.
   d) Enter a value for the **Quick Filter** parameter and click **Add Filter**.
3. To disable lazy search completely, do these steps:
   a) Click the **System Settings** on the **Admin** tab.
   b) In the **System Settings** window, remove any values from the **Default Search Limit** field.

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. Choose one of the following options:
   - Click the **Log Activity** tab.

- Click the **Network 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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** or **Network Activity** tabs to view partial or complete 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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**, **Network Activity**, and **Offenses** tabs, 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**, **Flow Search Group**, or **Offense Search Group** windows.

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

The **Event Search Group, Flow Search Group**, and **Offense Search Group** windows display the following parameters for each group.

Table 36. Search Group window parameters

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

The **Event Search Group**, **Flow Search Group**, and **Offense Search Group** window toolbars provide the following functions.

Table 37. Search Group window toolbar functions

Function	Description
New Group	To create a new search group, you can click **New Group**. See Creating a new search group.
Edit	To edit an existing search group, you can click **Edit**. See Editing a search group.
Copy	To copy a saved search to another search group, you can click **Copy**. See Copying a saved search to another group.

Remove	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 Removing a group or a saved search from a group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Select the group that you want 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. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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 the following groups from your system:

- Event Search Groups
- Flow Search Groups
- Offense Search Groups
- Other

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network 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**.

Search example: Daily employee reports

The following example describes how to use a complex advanced search query to see specific employee information.

For identity management purposes, you decide to generate a daily report of the user activity in QRadar. The report must include information about the employee, such as their user names, their serial number, their manager, and their activities.

An employee might have multiple user names in QRadar. You use the RESTful API to build a reference map that returns all associated user names to the employee's name, Global_User. For the serial number and the manager's name, you create another reference data set and add it to the reference map.

Employee activities can range from login failures to QRadar tasks, such as deleting objects. These events are recorded by QRadar. By specifying the frequency of the events in the map, you can gauge when suspicious activity occurs. You group the data by the employee's name and the event name, and then sort the data by the highest event frequency within a 24-hour time frame.

To see this daily report, you log in to QRadar Console. In the Advanced Search text box on the **Log Activity** tab, you type the following search query:

```
select REFERENCEMAP('GlobalID_Mapping', username) as Global_User, QIDNAME(qid) as 'Event
Name', count(*) as 'Event Count', FIRST(username) as UserId,
REFERENCETABLE('employee_data','SerialNum', Global_user) as 'Serial Number',
REFERENCETABLE('employee_data','Manager',Global_User) as Manager from events where
(Global_User IS NOT NULL) GROUP BY Global_user,'Event Name' ORDER BY
'Event Count' DESC last 1 DAYS
```

Chapter 11. Custom event and flow properties

IBM QRadar normalizes standard information that is parsed by the DSM, such as user names, IP addresses, and ports.

Some event sources send unique information that is not normalized. You can use custom properties to extract that data from the event or flow payload, and then use the non-normalized data in custom rules, searches, and reports.

The type of custom property that you create depends on the method that you want to use to define the non-normalized data in the payload.

Extraction-based properties

Create an extraction-based property when you want to use a regex or JSON expression to parse the property values from the event or flow payloads.

For example, you have a report that shows all the users who changed other user's permissions on an Oracle server. The report uses normalized data to show the list of users who made the permission changes and the number of changes they made. The user account that was changed is not normalized and cannot be shown in the report. You can create a regex-based custom property to extract this information from the logs, and then use the property in searches and reports.

When the event or flow is parsed, the expression pattern is tested against each payload until the pattern matches. The first pattern to match the event or flow payload determines the data to be extracted.

When you define custom regex patterns, follow the regex rules as defined by the Java programming language. To learn more about regex rules, you can view regex tutorials on the web.

Calculation-based properties

Create a calculation-based property when you want to do calculations on existing numeric event and flow properties. For example, you can create a calculation-based property that divides one numeric property by another numeric property to display a percentage value.

AQL-based properties

Create an AQL-based property when you want to combine multiple extraction and calculation-based properties into a single property. For example, you can use AQL-based custom properties to combine extraction-based URLs, virus names, or secondary user names into a single property.

```
CONCAT( 'Src=', sourceip, ' | ', 'User=', username, ' | ', 'Domain=',
DOMAINNAME(domainid) )
```

Note: The AQL expression can include AQL functions.

It does not support expressions that use SELECT, FROM, or database names.

You cannot use aggregate functions, such as SUM or GROUP, or other AQL-based custom

properties. © Copyright IBM Corp. 2012, 2021

Creating a custom property

Create a custom property to extract data that IBM QRadar does not typically show from the event or flow payloads. Custom properties must be enabled, and extraction-based custom properties must be parsed, before you can use them in rules, searches, reports, or for offense indexing.

Before you begin

QRadar includes a number of existing custom event properties that are not enabled or parsed by default. Ask your administrator to review the custom event property that you want to create to ensure that it does not exist.

To create custom event properties, you must have the **User Defined Event Properties** permission.

To create custom flow properties, you must have the **User Defined Flow Properties** permission. You must also set the **IPFIX Additional Field Encoding** field to **Payload** or **TLV and Payload**.

Users with administrative capabilities can create custom event and flow properties by selecting **Custom Event Properties** or **Custom Flow Properties** on the **Admin** tab.

You must configure a flow collector to export data to a flow processor. For more information, see Configuring the Flow Collector format.

About this task

Although multiple default custom properties might have the same name and the same log source, they can have different regex expressions, event names, or categories. For example, there are multiple custom

properties for Microsoft Windows Security Event Log called **AccountName**, but each one is defined by a unique regex expression.

Procedure

1. Click the **Log Activity** tab or the **Network Activity** tab.
2. If you are viewing the events or flows in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event or flow that contains the data that you want to extract, and then click **Extract Property**.
4. In the **Property Type Selection** pane, select the type of custom property that you want to create.
5. Configure the custom property parameters.

   Click the help icon ( ) to see information about the custom property parameters.
6. If you are creating an extraction-based custom property that is to be used in rules, search indexes, orforwarding profiles, ensure that the **Parse in advance for rules, reports, and searches** check box is selected.
7. Click **Test** to test the expression against the payload.
8. Click **Save**.

What to do next

"Modifying or deleting a custom property" on page 175

Related concepts

AQL search string examples

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Modifying or deleting a custom property

Edit a property when you want to change the property parameters, such as the regex expression or the log source type.

About this task

You can search for a specific property by using the **Search properties** field. The search is not casesensitive.

Make a copy of a custom property when you want to change it, and then save it using a different name.

To delete a property, you must first remove all dependencies to it. Deleting a custom property does not delete the indexed property fields from the Ariel database.

Procedure

1. Choose one of the following options:
   - To edit or delete a custom event property, click the **Log Activity** tab.
   - To edit or delete a custom flow property, click the **Network Activity** tab.
2. From the **Search** list box, select **Edit Search**.
3. Click **Manage Custom Properties**.
4. Select the property from the list, and click **Edit**, **Copy**, or **Delete**.
5. Make the required changes to the property, and then click **Save**.

Defining custom properties by using custom property expressions

Define a custom property for an event payload by using a custom property expression. Because JSON parsing begins when a valid JSON object is detected, the entire event does not need to be in JSON format. Similarly, LEEF and CEF parsing begins only when a valid LEEF/CEF message is detected within the event. Regex parsing runs through the entire payload.

About this task

IBM QRadar supports the following custom property expression types:

- Regex
- JSON
- LEEF
- CEF
- Name Value Pair
- Generic List
- XML

You can use different expressions to capture various custom properties for the same event. You can also use a combination of expression types to capture the same custom property if that property can be captured from multiple event formats.

Procedure

1. Log in to QRadar and click the **Admin** tab.
2. From the **Data Sources** section, click **Custom Event Properties**, and then click **Add**.
3. In the **Property Type Selection** section, select **Extraction Based**.
4. In the **Test Field**, enter the event payload that you want to use to test your custom property.
5. In the **Property Definition** section, complete the following steps:
   a) If you're adding an expression to an existing property, select **Existing Property** and select a property from the list.
   b) If you're defining a new property, select **New Property** and enter the name of the property.
   c) To use the property for rules, reports and searches, select the **Parse in advance for rules, reports, and searches** check box.

      You must select this check box to use the property for rules and indexes. Selecting the check box increases the efficiency of reports and searches, but you don't need to select it to use the property for reports and searches. When you select the check box, properties are parsed when the event is initially received and before it is stored. As a result, the loads are put on the event collection service.
   d) Select a **Field Type** for the property.

      If you choose IP as the type for your custom property, QRadar supports only IPv4.
   e) Optional: Enter a description for the property.
6. In the **Property Expression Definition** section, complete the following steps:
   a) Keep the **Enabled** check box selected; otherwise, clear the check box to disable the property.
   b) From the **Log Source Type** list, select a log source type for the property.
   c) If the expression is only evaluated against events for a specific log source, select the log source from the **Log Source** list. If you want it to be evaluated against all log sources, don't select.

d) If the expression is only evaluated against events with a specific event name or QID, click the **Event Name** and browse for a QID to associate the expression with.

e) If the expression is evaluated against any event with a specific low-level category, select **Category**, and select the **High Level Category** and then **Low Level Category** for the event.

Tip: If the expression is evaluated for all events of the selected log source type and log source, ensure that you set the **Low Level Category** and **High Level Category** to **Any**.

f) From the **Extraction using** field, select the extraction method to use for the property.

Table 38. Property extraction methods

Extraction method	Valid expression form	Example
Regex	Enter the regex and the capture group number.	

Table 38. Property extraction methods (continued)

Extraction method	Valid expression form	Example
JSON Keypath	A valid JSON expression is in the form: /"*<name of top-level field>*" For an event in a nested JSON format, a valid JSON expression is in the form: /"*<name of top-level field>*"/"*<name of sub-level field_1>*"...../"*<name of sub-level field_n>*" To extract the 'user' field, type /"user" in the **JsonKeypath** field. To extract just the 'last_name' value from the 'user' subobject, type this expression: /"user"/"last_name"	The following example is a simple case of an event for a flat JSON record: {"action": "login", "user": "Firstname Lastname"} The following example is a complex case of an event for a JSON record with nested objects: { "action": "login", "user": { "first_name": "Firstname", "last_name": "Lastname" } }

Table 38. Property extraction methods (continued)		
Extraction method	**Valid expression form**	**Example**

LEEF Key	Valid LEEF expressions are in the form of either a single key reference, or a special LEEF header field reference.
	To extract the 'usrName' property, type usrName in the **LEEF Key** field.
	The possible keys that can be extracted in these examples are:
	• devTimeFormat
	• devTime
	• usrName
	• name
	• authType
	• src
	To extract a header key property, type the key in the following format in the **LEEF Key** field:
	`$eventid$`
	The LEEF header values can be extracted by using the following expressions:
	• $leefversion$
	• $vendor$
	• $product$
	• $version$
	• $eventid$
		The following example is a simple case of an event that is formatted in LEEF V1.0:
		`LEEF:1.0|ABC Company| SystemDefender|1.13| console_login| devTimeFormat=yyyy-MMdd'T'HH:mm:ss.SSSZ devTime=2017-10-18T11:26:03.060+0 200 usrName=flastname name=Firstname Lastname authType=interactivePassword src=192.168.0.1`
		The following example is a simple case of an event that is formatted in LEEF V2.0 with the caret (^) separator character, and contains the same keys as the LEEF V1.0 example:
		`LEEF:2.0|ABC Company| SystemDefender|1.13| console_login|^| devTimeFormat=yyyyMMdd'T'HH:mm:ss.SSSZ^ devTime=2017-10-18T11:26:03.060+0 200^usrName= flastname^name=Firstname Lastname ^authType=interactivePassword^src =192.168.0.1`

Table 38. Property extraction methods (continued)		
Extraction method	**Valid expression form**	**Example**
CEF Key	Valid CEF expressions are in the form of either a single key	The following example shows an event that is in CEF format:

	reference, or a special CEF header field reference. To extract the 'cs1' property, type cs1 in the **CEF Key** field. The possible keys that can be extracted in the example are: • start • duser • cs1 • cs1Label • cs2 • cs2Label • src To extract a header key property, type the key in the following format in the **CEF Key** field: `$id$` The CEF header values can be extracted by using the following expressions: • $cefversion$ • $vendor$ • $product$ • $version$ • id • $name$ • $severity$	`CEF:0|ABC Company|SystemDefender| 1.13|console_login| Console Login|1|start=Oct 18 2017 11:26:03 duser=flastname cs1=Firstname Lastname cs1Label=Person Name cs2=interactivePassword cs2Label=authType src=192.168.0.1`
Name Value Pair Key	Valid Name Value Pair expressions are in the form of a single key reference.	The following example shows an event that is in Name Value Pair format: `Company=ABC Company;Product=SystemDefender; Version=1.13;EventID=console_logi n; Username=jsmith;Name=John Smith;authType=interactivePasswor d;`

Table 38. Property extraction methods (continued)

Extraction method	Valid expression form	Example
Generic List Keypath	Valid Generic List expressions are in the form of a	The following example shows an event that is in Generic List format:

	$<number> notation. For example, $0 represents the first property in the list, $1 is the second property, and so on.	ABC Company;1.13;console_login;jsmith ; John Smith;interactivePassword;
XML Key	Valid XML expressions are in the form of a single key reference. Enter the path to the XML field that you want to use to populate the property's value. An XML key path must begin with a forward slash (/) to indicate the root of the XML object, and be followed by one or more XML field names within double quotation marks.	The following example shows an event that is in XML format: <EPOEvent><MachineInfo> <MachineName>NEPTUNE</ MachineName> <MachineName>VALUE23</ MachineName><AgentGUID> 9B-B5-A6-A8-37-B3</ AgentGUID><IPAddress someattrib="someattribvalue"> 192.0.2.0</IPAddress> <OSName>Windows 7</ OSName><UserName>I am a test user</UserName></ MachineInfo></EPOEvent>

g) If you chose the Numeric **Field Type** in the **Property Definition** section, select a number format in the **Extracted Number Format** field in the **Format** section to define any digit group separators for the locale of the custom property.

h) If you chose the Date/Time **Field Type** in the **Property Definition** section, enter a format in the **Extracted Date/Time Format** and **Locale** fields in the **Format** section to define the date and time for the locale of the custom property.

i) Click **Test** to test the property expression definition.

7. Click **Save**.

Use case: Create a report that uses event data that is not normalized

You can use a custom property to extract data that is not normalized from a payload, and use that data to build a report. For example, you can build a report that is based on the interface information that is in Cisco ASA firewall deny messages.

In this example, we'll use the following sample Cisco ASA firewall events to demonstrate how to extract the interface value from the event payload, and then build a report that uses that data.

```
<162>Sep 02 2014 11:49:41: %ASA-2-106001: Inbound TCP connection denied from 10.10.10.128/58826 to
10.11.11.11/9100 flags SYN on interface External
<162>Sep 02 2014 11:49:40: %ASA-2-106001: Inbound TCP connection denied from 10.10.10.128/58826 to
10.11.11.11/9100 flags SYN on interface Loopback
<162>Sep 02 2014 11:49:17: %ASA-2-106001: Inbound TCP connection
denied from 10.10.10.128/58821 to 10.11.11.11/9100 flags SYN on interface Internal
```

1. Create the custom property.

   In the sample events above, you can see that the event payload includes the word interface followed by the value that you want to extract. To capture the interface information from the events above, create an extraction-based custom property and configure it to use the regex expression interface\s(.*)\b.

   To ensure that the new custom property is available to use in a search, select the **Parse in advance for rules, reports, and searches** check box, and enable the custom property.

2. Create a search, and in the **Group By** field, select the new custom event property.

To ensure that the search results include only Cisco ASA events, add the log source as a quick filter option in the search parameters. Save the search criteria so that you can use it in a report. Assign the saved search to a group to make it easier to find later.

3. Create a report, and configure the graph content to use the new saved search.

   If the report was not configured to run after saving, you can run the report immediately by selecting **ActionsRun Report**.

Chapter 12. Rules

Rules, sometimes called correlation rules are applied to events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates response.

What are rules?

Custom rules test events, flow, and offenses to detect unusual activity in your network. You create new rules by using AND and OR combinations of existing rule tests. Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur in your network. Anomaly detection rules require a saved search that is grouped around a common parameter.

What are building blocks?

A building block is a collection of tests that don't result in a response or an action.

A building block groups commonly used tests to build complex logic so that it can be reused in rules. A building block often tests for IP addresses, privileged user names, or collections of event names. For example, a building block can include the IP addresses of all DNS servers. Rules can then use this building block.

QRadar has default rules and you can also download more rules from the IBM Security App Exchange to create new rules.

How do rules work?

QRadar Event Collectors gather events from local and remote sources, normalize these events, and classify them into low-level and high-level categories. For flows, QRadar QFlow Collectors read packets from the wire or receive flows from other devices and then converts the network data to flow records. Each Event Processor processes events or flow data from the QRadar Event Collectors. Flow Processors examine and correlate the information to indicate behavioral changes or policy violations. The custom rules engine (CRE) processes events and compares them against defined rules to search for anomalies. When a rule condition is met, the Event Processor generates an action that is defined in the rule response. The CRE tracks the systems that are involved in incidents, contributes events to offenses, and generates notifications.

How is an offense created from a rule?

QRadar creates an offense when events, flows, or both meet the test criteria that is specified in the rules.

QRadar analyzes the following information:

- Incoming events and flows
- Asset information
- Known vulnerabilities

The rule that created the offense determines the offense type.

The magistrate prioritizes the offenses and assigns the magnitude value based on several factors, including number of events, severity, relevance, and credibility.

Note: Building blocks are tested before rules are tested.

For example, you have a building block that is defined to trigger an offense on high magnitude events. The log activity can show that there were high magnitude events, but no offense was triggered. This can happen because when the building block was tested, the events was not at high magnitude. The magnitude of the event did not increase until the rules were tested.

© Copyright IBM Corp. 2012, 2021

One solution is to set a rule to check for the different in Severity, Credibility, and Relevance rather than to use a building block.

Custom rules

IBM QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

What are custom rules?

Customize default rules to detect unusual activity in your network.

Rule types

Each of the event, flow, common, and offense rule types test against incoming data from different sources in real time. There are multiple types of rule tests. Some check for simple properties from the data set. Other rule tests are more complicated. They track multiple, event, flow, and offense sequences over a period of time and use "counter" that is on one or more parameters before a rule response is triggered.

Event rules
: Test against incoming log source data that is processed in real time by the QRadar Event Processor. You create an event rule to detect a single event or event sequences. For example, to monitor your network for unsuccessful login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, you create an event rule. It is common for event rules to create offenses as a response.

Flow rules
: Test against incoming flow data that is processed by the QRadar Flow Processor. You can create a flow rule to detect a single flow or flow sequences. It is common for flow rules to create offenses as a response.

Common rules
: Test against event and flow data. For example, you can create a common rule to detect events and flows that have a specific source IP address. It is common for common rules to create offenses as a response.

Offense rules
: Test the parameters of an offense to trigger more responses. For example, a response generates when an offense occurs during a specific date and time. An offense rule processes offenses only when changes are made to the offense. For example, when new events are added, or the system scheduled the offense for reassessment. It is common for offense rules to email a notification as a response.

Managing rules

You can create, edit, assign rules to groups, and delete groups of rules. By categorizing your rules or building blocks into groups, you can efficiently view and track your rules. For example, you can view all rules that are related to compliance.

Domain-specific rules

If a rule has a domain test, you can restrict that rule so that it is applied only to events that are happening within a specified domain. An event that has a domain tag that is different from the domain that is set on, the rule does not trigger a response.

To create a rule that tests conditions across the entire system, set the domain condition to **Any Domain**.

Rule conditions

Most rule tests evaluate a single condition, like the existence of an element in a reference data collection or testing a value against a property of an event. For complex comparisons, you can test event rules

by building an Ariel Query Language (AQL) query with WHERE clause conditions. You can use all of the WHERE clause functions to write complex criteria that can eliminate the need to run numerous individual tests. For example, use an AQL WHERE clause to check whether inbound SSL or web traffic is being tracked on a reference set.

You can run tests on the property of an event, flow, or offense, such as source IP address, severity of event, or rate analysis.

With functions, you can use building blocks and other rules to create a multi-event, multi-flow, or multioffense function. You can connect rules by 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.

Related information
How do rules perform tests on events, flows, and offenses? (Security Learning Academy course)

Creating a custom rule

IBM QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

Before you begin

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

About this task

When you define rule tests, test against the smallest data possible. Testing in this way helps rule test performance and ensures that you don't create expensive rules. To optimize performance, start with broad categories that narrow the data that is evaluated by the rule test. For example, start with a rule test for a specific log source type, network location, flow source, or context (R2L, L2R, L2L). Any mid-level tests might include IP addresses, port traffic, or any other associated test. The rule should test payload and regex expressions last.

Similar rules are grouped by category. For example, Audit, Exploit, DDoS, Recon, and more. When you delete an item from a group, the rule or building block is only deleted from the group; it remains available on the **Rules** page. When you delete a group, the rules or building blocks of that group remain available on the **Rules** page.

Procedure

1. From the **Offenses**, **Log Activity**, or **Network Activity** tabs, click **Rules**.
2. From the **Display** list, select **Rules** to create a new rule.
3. Optional: From the **Display** list, select **Building Blocks** to create a new rule by using building blocks.
4. From the **Actions** list, select a rule type.

   Each rule type tests against incoming data from different sources in real time. For example, event rules test incoming log source data and offense rules test the parameters of an offense to trigger more responses.
5. In the **Rule Wizard** window, select the **Skip this page when running this rules wizard** checkbox and click **Next**.

If you select the **Skip this page when running this rules wizard** checkbox, the **Welcome** page does not appear each time that you start.

6. On the **Rule Test Stack Editor** page, in the **Rule** pane, type a unique name that you want to assign to this rule in the **Apply** text box.
7. From the list box, select **Local** or **Global**.
   - If you select **Local**, all rules are processed on the Event Processor on which they were received and offenses are created only for the events that are processed locally.
   - If you select **Global**, all matching events are sent to the QRadar Console for processing and therefore, the QRadar Console uses more bandwidth and processing resources.

   Learn more about Local and Global rules:

   Global rule tests

   Use global rules to detect things like "multiple user login failures" where the events from that user might appear on multiple Event Processors. For example, if you configured this rule for 5 login failures in 10 minutes from the same user name, and set as a **Local** rule, all 5 of those login failures must appear on the same Event Processor. Therefore, if 3 login failures were on one Event Processor and 2 were on another, no offense is generated. However, if you set this rule to **Global**, it generates an offense.
8. From the **Test Group** list, select one or more tests that you want to add to this rule. The CRE evaluates rule tests line-by-line in order. The first test is evaluated and when true, the next line is evaluated until the final test is reached.

   If you want to select the **when the event matches this AQL filter query** test for a new event rule, click the add **(+)** icon. In the **Rule** pane, click **This** and enter an AQL WHERE clause query in the **Enter an AQL filter query** text box.

   Learn more about using rules for events that are not detected:

   The following rule tests can be triggered individually, but rule tests in the same rule test stack are not acted upon.

   - **when the event(s) have not been detected by one or more of these log source types for this many seconds**
   - **when the event(s) have not been detected by one or more of these log sources for this many seconds**
   - **when the event(s) have not been detected by one or more of these log source groups for this many seconds**

   These rule tests are not activated by an incoming event, but instead are activated when a specific event is not seen for a specific time interval that you configured. QRadar uses a *watcher task* that periodically queries the last time that an event was seen (last seen time), and stores this time for the event, for each log source. The rule is triggered when the difference between this last seen time and the current time exceeds the number of seconds that is configured in the rule.
9. To export the configured rule as a building block to use with other rules, click **Export as Building Block**.
10. On the **Rule Responses** page, configure the responses that you want this rule to generate.

    Learn more about rule response page parameters:

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters

Parameter	Description

Bypass further rule correlation event	Forces the matched event or flow to bypass all other rules in the rule engine and prevents it from creating an offense. The event is written to storage for searching and reporting.
Dispatch New Event	Select this check box to dispatch a new event in addition to the original event or flow, which is processed like all other events in the system. Dispatches a new event with the original event, and 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.

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters (continued)

Parameter	**Description**
Severity	The severity level that you want to assign to the event, where 0 is the lowest and 10 is the highest. The severity is displayed in the **Annotation** pane of the event details.
Credibility	The credibility that you want to assign to the log source. For example, is the log source noisy or expensive? The range is 0 (lowest) to 10 (highest) and the default is 10. Credibility is displayed in the **Annotation** pane of the event details.
Relevance	The relevance that you want to assign to the weight of the asset. For example, how much do you care about the asset? The range is 0 (lowest) to 10 (highest) and the default is 10. Relevance is displayed in the **Annotation** pane of the event details.
Email	To change the **Email Locale** setting, select **System Settings** on the **Admin** tab.
Enter email addresses to notify	Use a comma to separate multiple email addresses.
SNMP Trap	Enable this function 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. You can access the MIB from /opt/qradar/conf/Q1LABS-MIB.txt.
Send to Local SysLog	If you want to log the event or flow locally, select this check box. By default, this check box is clear. **Note:** Only normalized events can be logged locally on an appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.

Send to Forwarding Destinations	If you want to log the event or flow on a forwarding destination, select this check box. 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. To add, edit, or delete a forwarding destination, click the **Manage Destinations** link.
Notify	Displays 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.

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters (continued)

Parameter	**Description**
Add to Reference Set	Adds events that are generated as a result of this rule to a reference set. You must be an administrator to add data to a reference set. To add data to a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to add. b. From the second list, select the reference set to which youwant to add the specified data.
Add to Reference Data	To use this rule response, you must create the reference data collection.
Remove from Reference Set	If you want this rule to remove data from a reference set, select this check box. To remove data from a reference set: a. From the first list box, select the property of the event or flow that you want to remove. Options include all normalized or custom data. b. From the second list box, select the reference set from whichyou want to remove the specified data. The **Remove from Reference Set** rule response provides the following function: **Refresh** Click **Refresh** to refresh the first list box to ensure that the list is current.
Remove from Reference Data	To use this rule response, you must have a reference data collection.

Execute Custom Action	You can write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
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	Configures the frequency in which you want this rule to respond.

Table 39. Event , Flow and Common Rule, and Offense Rule Response page parameters (continued)

Parameter	**Description**
Offense Name	If you want the **Event Name** information to contribute to the name of the offense, select the **This information should contribute to the name of the offense** option. If you want the configured **Event Name** to be the name of the offense, select the **This information should set or replace the name of the offense** option. **Note:** This option does not rename existing offenses. To rename an existing offense, you must use the Offense Rule option **This information should set or replace the name of the offense**.

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 1, 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
```

What to do next

To test your rules, run Chapter 13, “Historical correlation,” on page 203.

To verify that the event triggers the rule test based on your building block, you can create an email response. See “Sending email notifications” on page 42.

Related information

Managing Custom Rules in QRadar SIEM
How is Custom Rule Engine capacity calculated? (Security Learning Academy course)

Configuring an event or flow as false positive

You might have legitimate network traffic that triggers false positive flows and events that makes it difficult to identify true security incidents. You can prevent events and flows from correlating into offenses by configuring them as false positives.

Procedure

1. From the, **Log Activity**, or **Network Activity** tabs, click the pause on the upper right to stop real-time streaming of events or flows.
2. Select the event that you want to tune.
3. Click **False Positive**.
4. Select an event or flow property option.
5. Select a traffic direction option.
6. Click **Tune**.

Results

The event or flow that matches the specified criteria will no longer correlates into offenses. To edit false positive tuning, use the **User-BB_FalsePositive: User Defined Positive Tunings building** block in the **Rules** section on the **Offenses** tab.

Anomaly detection rules

Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur in your network.

Anomaly detection rules require a saved search that is grouped around a common parameter, and a time series graph that is enabled. Typically the search needs to accumulate data before the anomaly rule returns any result that identifies patterns for anomalies, thresholds, or behavior changes.

Anomaly rules

Test event and flow traffic for changes in short-term events when you are comparing against a longer timeframe. For example, new services or applications that appear in a network, a web server crashes, firewalls that all start to deny traffic.

Example: You want to be notified when one of your firewall devices is reporting more often than it usually does because your network might be under attack. You want to be notified when you receive twice as many events in 1 hour. You follow these steps:

1. Create and save a search that groups by log source, and displays only the count column.
2. Apply the saved search to an anomaly rule, and add the rule test, **and when the average value (per interval) of count over the last** 1 hour **is at least** 100% **different from the average value (per interval) of the same property over the last** 24 hours.

Threshold rules

Test events or flows for activity that is greater than or less than a specified range. Use these rules to detect bandwidth usage changes in applications, failed services, the number of users connected to a VPN, and detecting large outbound transfers.

Example: A user who was involved in a previous incident has large outbound transfer.

When a user is involved in a previous offense, automatically set the Rule response to add to the Reference set. If you have a watch list of users, add them to the Reference set. Tune acceptable limits within the Threshold rule.

A reference set, WatchUsers, and Key:username are required for your search.

Complete the following search, and then apply it to a Threshold rule.

```
select assetuser(sourceip, now()) as 'srcAssetUser',
Applicationname(applicationid)as 'AppName', long(sum(sourcebytes
+destinationbytes)) as 'flowsum' from flows where flowdirection = 'L2R' and
REFERENCESETCONTAINS('Watchusers', username)group by 'srcAssetUser', applicationid order by 'flowsum' desc last 24 hours
```

Behavioral rules

Test events or flows for volume changes that occur in regular patterns to detect outliers. For example, a mail server that has an open relay and suddenly communicates with many hosts, or an IPS (intrusion protection system) that starts to generate numerous alert activities.

A behavioral rule learns the rate or volume of a property over a pre-defined season. The season defines the baseline comparison timeline for what you're evaluating. When you set a season of 1 week, the behavior of the property over that 1 week is learned and then you use rule tests to alert you to any significant changes.

After a behavioral rule is set, the season adjusts automatically. When the data in the season is learned, it is continually evaluated so that business growth is profiled within the season; you do not have to change your rules. The longer a behavioral rule runs, the more accurate it becomes. You can then adjust the rule responses to capture more subtle changes.

The following table describes the behavioral rule test parameter options.

Table 40. Behavioral rule test definitions

Rule test parameter	Description
Season	The most important value. The season defines the baseline behavior of the property that you are testing and which the other rule tests use. To define a season, consider the type of traffic that you are monitoring. For example, for network traffic or processes that include human interaction, 1 week is a good season timeframe. For tracking automated services where patterns are consistent, you might want to create a season as short as 1 day to define that pattern of behavior.
Current traffic level	Weight of the original data with seasonal changes and random error accounted for. This rule test asks the question, "Is the data the same as yesterday at the same time?" The weight must be in the range of 1 to 100. A higher value places more weight on the previously recorded value.

Current traffic trend	Weight of changes in the data for each time interval. This rule test asks the question, "How much does the data change when it compares this minute to the minute before?" The weight must be in the range of 1 to 100. A higher value places more weight on traffic trends than the calculated behavior.
Current traffic behavior	Weight of the seasonal effect for each period. This rule test asks the question, "Did the data increase the same amount from week 2 to week 3, as it did from week 1 to week 2?" The weight must be in the range of 1 to 100. A higher value places more weight on the learned behavior.
Predicted value	Use predicted values to scale baselines to make alerting more or less sensitive. The sensitivity must be in the range of 1 to 100. A value of 1 indicates that the measured value cannot be outside the predicted value. A value of 100 indicates that the traffic can be more than four times larger than the predicted value.

The forecast for value from $(n+1)^{th}$ interval is calculated by using the following formula:

$$F_{n+1} = B_n + T_n + T_{n+1-s}$$

Where F is the predicted value, B is the base value for interval n, T is the trend value for interval n, and T is the trend value for season intervals ago and s is the number of intervals within the season.

The base value is calculated by using the following formula:

$$B_{n+1} = (0.2 + 0.3*(<\textit{Current traffic level}> / 100.0))*(value_{n+1} – T_{n+1-s}) + (1 – (0.2 + 0.3*(<\textit{Current traffic level}> / 100.0)))*T_n$$

The trend value is calculated by using the following formula:

$$T_{n+1} = (0.2 + 0.3*(<\textit{Current traffic trend}> / 100.0))*(B_{n+1} - B_n) + (1 - (0.2 + 0.3*(<\textit{Current traffic trend}> / 100.0)))*T_n$$

Smoothed deviation D is calculated by using the following formula:

$$D_{n+1} = (0.2 + 0.3*(<\textit{Current traffic behavior}> / 100.0))*|value_{n+1} – F_{n+1}| + (1 – (0.2 + 0.3*(<\textit{Current traffic behavior}> / 100.0)))*D_{n+1-s}$$

The behavioral rule produces an alert for the interval if the following expression is false:

$$F – (1 + (\textit{sensitivity} / 100.0)*3)*D <= value <= F + (1 + (\textit{sensitivity} / 100.0)*3)*D$$

During the first season, the behavioral rule learns for future calculations and doesn't produce any alerts.

Creating an anomaly detection rule

Anomaly detection rules test the result of saved flow or event searches to search for unusual traffic patterns that occur in your network. Behavioral rules test event and flow traffic according to "seasonal" traffic

levels and trends. Threshold rules test event and flow traffic for activity less than, equal to, or greater than a configured threshold or within a specified range.

Before you begin

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 Activity Maintain Custom Rules** role permission.

To manage default and previously created anomaly detection rules, use the **Rules** page on the **Offenses** tab.

About this task

When you create an anomaly detection rule, the rule is populated with a default test stack, based on your saved search criteria. 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.

An anomaly detection rule tests the selected accumulated property for each event or flow group separately. For example, if the selected accumulated value is **UniqueCount(sourceIP)**, the rule tests each unique source IP address for each event or flow group.

The **Test the [Selected Accumulated Property] value of each [group] separately** option is dynamic. The **[Selected Accumulated Property]** value depends on the option that 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** or **Network Activity** tab.
2. Perform an aggregated search.

   You can add a property to the **group by** in a new historical search or select a property from the **Display** list on the current search page.
3. On the search result page, click **Configure**, and then configure the following options:
   a) Select a property from the **Value to Graph** list.
   b) Select **time series** as the chart type from the **Value to Graph** list
   c) Enable the **Capture Time Series Data** check box.
   d) Click **Save**, and then enter a name for your search.
   e) Click **OK**.
   f) Select last 5 minutes from the **Time Range** list, while you wait for the time series graph to load.

   You must have time series data for the property that you selected in the **Value to Graph** list to run a rule test on that accumulated property.
4. From the **Rules** menu, select the rule type that you want to create.
   - Add Anomaly Rule
   - Add Threshold Rule

- Add Behavioral Rule

5. On the **Rule Test Stack Editor** page, in the **enter rule name here** field, type a unique name that you want to assign to this rule.
6. To apply your rule by using the default test, select the first rule in the anomaly **Test Group** list.

   You might need to set the accumulated property parameter to the property that you selected from the **Value to Graph** list that you saved in the search criteria. If you want to see the result sooner, set the percentage to a lower value, such as 10%. Change **last 24 hours** to a lesser time period, such as 1 hour. Because an anomaly detection tests on aggregated fields in real time to alert you of anomalous network activity, you might want to increase or decrease events or flows in your network traffic.
7. Add a test to a rule.
   a) To filter the options in the **Test Group** list, type the text that you want to filter for in the **Type to filter** field.
   b) From the **Test Group** list, select the type of test that you want to add to this rule.
   c) To identify a test as an excluded test, click **and** at the beginning of the test in the Rule pane. The **and** is displayed as **and not**.
   d) Click the underlined configurable parameters to customize the variables of the test.
   e) From the dialog box, select values for the variable, and then click **Submit**.
8. To test the total selected accumulated properties for each event or flow group, disable **Test the [Selected Accumulated Property] value of each [group] separately**.
9. In the groups pane, enable the groups you want to assign this rule to.
10. In the **Notes** field, type any notes that you want to include for this rule, and then Click **Next**.
11. On the **Rule Responses** page, configure the responses that you want this rule to generate.

    Learn more about rule response page parameters for anomaly detection rules:

    The following table provides the **Rule Response** page parameters if the rule type is Anomaly.

Table 41. Anomaly Detection Rule Response page parameters

Parameter	Description
Dispatch New Event	Specifies that this rule dispatches a new event with the original event or flow, which is processed like all other events in the system. By default, this check box is selected and cannot be cleared.

Offense Naming	If you want the Event Name information to contribute to the name of the offense, select the **This information should contribute to the name of the associated offense(s)** option. If you want the configured Event Name to contribute to the offense, select the **This information should set or replace the name of the associated offense(s)**. **Note:** After you replace the name of the offense, the name won't change until the offense is closed. For example, if an offense is associated with more than one rule, and the last event doesn't trigger the rule that is configured to override the name of the offense, the offense's name won't be updated by the last event. Instead, the offense name remains the name that is set by the override rule.
Severity	The severity level that you want to assign to the event. The range is 0 (lowest) to 10 (highest) and the default is 5. The Severity is displayed in the Annotations pane of the event details.
Credibility	The credibility that you want to assign to the log source. For example, is the log source noisy or expensive? Using the list boxes, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Credibility is displayed in the Annotations pane of the event details.
Relevance	The relevance that you want to assign to the weight of the asset. For example, how much do you care about the asset? Using the list boxes, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Relevance is displayed in the Annotations pane of the event details.
Ensure that the dispatched event is part of an offense	As a result of this rule, the event is forwarded to the magistrate. If an offense exists, this event is added. If no offense was created on the Offenses tab, a new offense is created.
Notify	Events that generate as a result of this rule are displayed in the System Notifications item in the **Dashboard** tab. If you enable notifications, configure the **Response Limiter** parameter.
Send to Local SysLog	Select this check box if you want to log the event or flow locally. By default, the check box is clear. **Note:** Only normalized events can be logged locally on a QRadar appliance. If you want to send raw event data, you must use the **Send to Forwarding Destinations** option to send the data to a remote syslog host.

Table 41. Anomaly Detection Rule Response page parameters (continued)

Parameter	**Description**

Add to Reference Set	Adds events that are generated as a result of this rule to a reference set. You must be an administrator to add data to a reference set. To add data to a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to add. b. From the second list, select the reference set to which youwant to add the specified data.
Add to Reference Data	To use this rule response, you must create the reference data collection.
Remove from Reference Set	If you want this rule to remove data from a reference set, select this check box. To remove data from a reference set, follow these steps: a. From the first list, select the property of the event or flow that you want to remove. b. From the second list, select the reference set from which youwant to remove the specified data.
Remove from Reference Data	To use this rule response, you must have a reference data collection.
Execute Custom Action	You can write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. Select this check box and select a custom action from the **Custom action to execute** list. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
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 offense information about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

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 1, 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
```

12. Click **Next**.
13. Click **Finish**.

Configuring a rule response to add data to a reference data collection

Set up rules that use reference data to alert you to suspicious activity. For example, include a list of privileged users into reference data and then set up a rule that is triggered to alert you when privileged user anomalies occur.

Before you begin

Before you send data to a reference set, your QRadar administrator must create the reference set.

About this task

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 that are 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 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 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 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 that are 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.

Procedure

1. Create the reference data collection by using the **Reference Set Management** widget on the **Admin** tab.

   You can also create a reference data collection by using the ReferenceDataUtil.sh script.

2. Create a rule by using the **Rules** wizard.
3. Create a rule response that sends data to a reference data collection. You can add the data as eithershared data or domain-specific data.

   Learn more about Add to Reference Data parameters:

   Add to a Reference Map
   Sends 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
   Sends 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
   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
   Sends 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.

Editing building blocks

You can edit any of the default building blocks to use it in multiple rules or to build complex rules or logic. You can save a group of tests as building blocks for use with 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 **Offenses** or **Network Activity tab**.
2. Click **Rules**.
3. From the **Display** list, 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.
8. Click **Finish**.

Related information
Overview of Building Blocks in QRadar SIEM

Rule performance visualization

Rule performance visualization extends the current logging around performance degradation and the expensive custom rules in the QRadar pipeline. With rule performance visualization, you can easily determine the efficiency of rules in the QRadar pipeline, directly from the **Rules** page.

Note: You must be an Administrator to turn on rule performance visualization. After rule performance visualization is turned on, users can view performance metrics for rules. For more information about turning on rule performance visualization, see the *IBM QRadar Administration Guide*.

When rule performance visualization is turned on, the **Performance** column is added to the **Rules** page. The **Performance** column is blank until a performance issue occurs in the custom rule engine.

Performance ▲	Rule Name	Group	Rule Category
	Devices with High	Anomaly	Custom Rule
	This rule has not yet had a detailed analysis.		Custom Rule
	Anomaly: Excessiv...	Recon	Custom Rule
	Excessive Firewall...	Anomaly	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule
	AssetExclusion: E...	Asset Reconciliati...	Custom Rule

*Figure 11. Performance column on the **Rules** page*

When events or flows are routed to storage, QRadar begins collecting metrics on enabled rules for efficiency measures. Metrics are collected on all event, common, and flow rules. When you save rule updates, the metrics are cleared for the rules that you updated to avoid any confusion around performance and updated rules. This option is configurable by an Administrator.

You can sort rules by their performance metrics and identify the more expensive rules. When you review the rules, you can adjust the tests to optimize each rule, and reduce the load on the system.

With rule performance visualization, you see how expensive the rules are. QRadar operations teams can monitor any expensive rules and ensure that they do not cause future performance issues.

By having rules run efficiently, the workload on the system can decrease. Over time, this efficiency can help QRadar avoid any performance degradations around rules, which cause rules to bypass rule correlation. As a result, potential suspect activity might not trigger a notification, potentially missing future security-related issues.

For more information about tuning rules, see the *IBM QRadar Tuning Guide*.

View the metrics for a rule

You can view the metrics for a rule from the **Rules** page when you move the mouse pointer over the colored bars in the **Performance** column, and in the **Performance Analysis** textbox, which is in the lower-right corner of the **Rules** page. You can also view the metrics for a rule in the **Rule Wizard** when you edit a rule. The timestamp in the **Performance Analysis** textbox shows when the metrics for the rule were updated. For more information about creating rules, see the Rules topic.

From the **Network Activity** tab or the **Log Activity** tab, click **Rules** to display the **Rules** page. Double-click a rule to open the **Rule Wizard**.

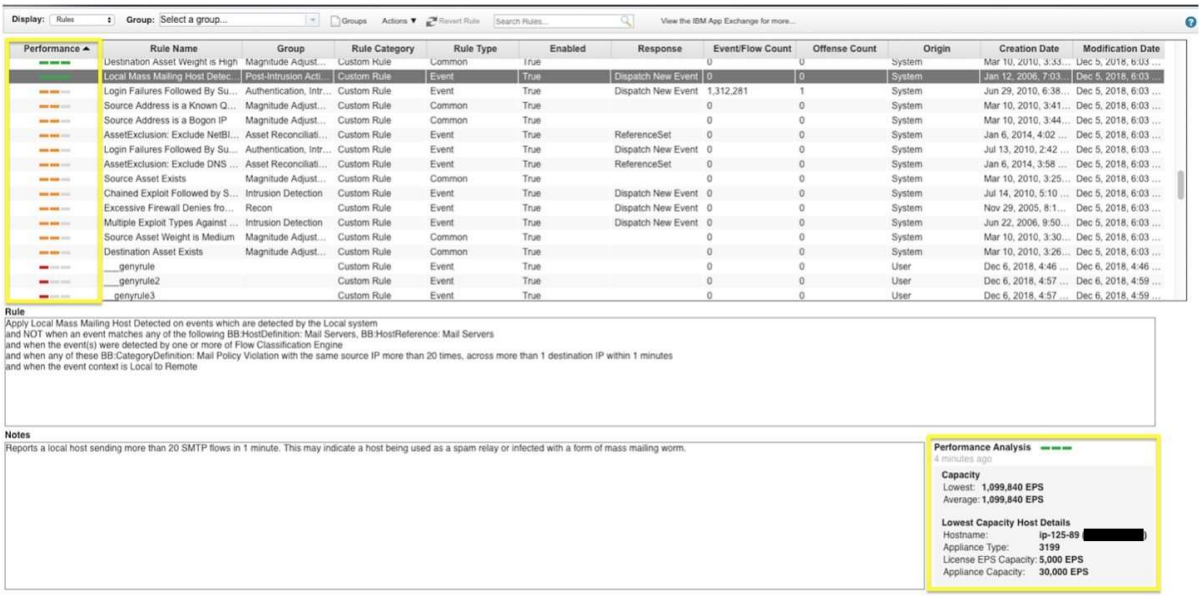


*Figure 12. Performance Analysis on the **Rules** page*

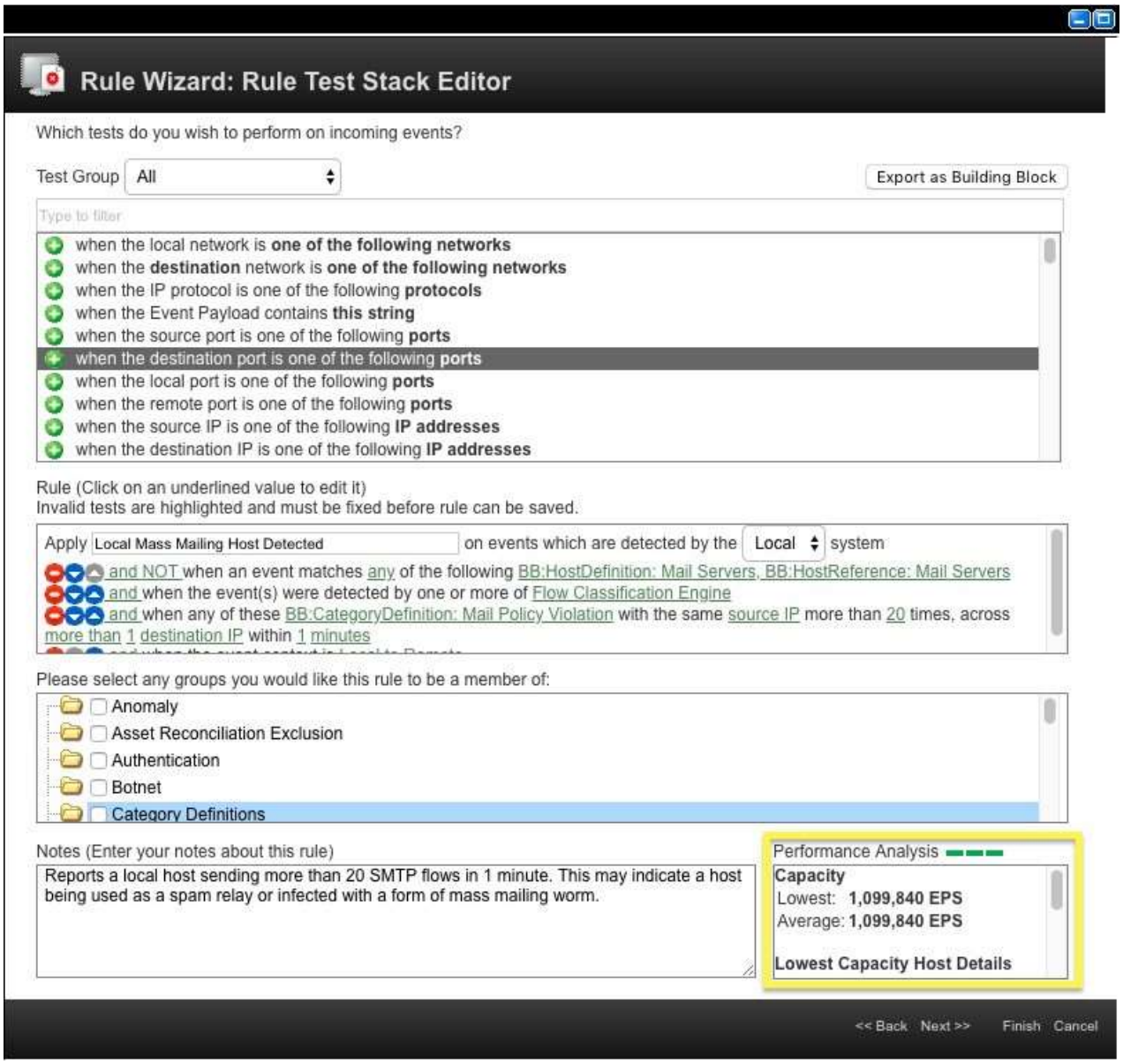


*Figure 13. Performance Analysis in the **Rule Wizard***

Colors and bars in the Performance column on the Rules page

The number of bars that display is a visual aid for color blindness.

One red bar

The rule is under-performing and needs to be tuned. The EPS/FPS throughput for this rule is below the lower limit. Open the rule and tune the tests.

Two orange bars

The rule might need some tuning.

Three green bars

The rule has a high throughput above the upper limit of the EPS/FPS threshold.

Note: The colors and number of bars can't be changed. The definition of a rule that is under-performing is configurable by an Administrator.

The following image shows the default **Custom Rule Settings** in QRadar.

Figure 14. ***Custom Rule Settings***

For more information about tuning rules, see the Custom" rule testing order" topic in the *IBM QRadar Tuning Guide*.

Related concepts

"Rules" on page 183

Rules, sometimes called correlation rules are applied to events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates response.

Chapter 13. Historical correlation

Use historical correlation to run past events and flows through the custom rules engine (CRE) to identify threats or security incidents that already occurred.

Restriction: You cannot use historical correlation in IBM QRadar Log Manager. For more information about the differences between IBM QRadar SIEM and IBM QRadar Log Manager, see Chapter 2, "Capabilities in your IBM QRadar product," on page 5.

By default, an IBM QRadar SIEM deployment analyzes information that is collected from log sources and flow sources in near real-time. With historical correlation, you can correlate by either the start time or the device time. *Start time* is the time that the event was received by QRadar. *Device time* is the time that the event occurred on the device.

Historical correlation can be useful in the following situations:

Analyzing bulk data
If you bulk load data into your QRadar deployment, you can use historical correlation to correlate the data against data that was collected in real-time. For example, to avoid performance degradation during normal business hours, you load events from multiple log sources every night at midnight. You can use historical correlation to correlate the data by device time to see the sequence of network events as they occurred in the last 24 hours.

Testing new rules
You can run historical correlation to test new rules. For example, one of your servers was recently attacked by new malware for which you do not have rules in place. You can create a rule to test for that malware. Then, you can use historical correlation to check the rule against historical data to see whether the rule would trigger a response if it were in place at the time of the attack. Similarly, you can use historical correlation to determine when the attack first occurred or the frequency of the attack. You can continue to tune the rule and then move it into a production environment.

Re-creating offenses that were lost or purged
If your system lost offenses because of an outage or other reason, you can re-create the offenses by running historical correlation on the events and flows that came in during that time.

Identifying previously hidden threats
As information becomes known about the latest security threats, you can use historical correlation to identify network events that already occurred but did not trigger an event. You can quickly test for threats that have already compromised your organization's system or data.

Historical correlation overview

You configure a historical correlation profile to specify the historical data that you want to analyze and the rule set that you want to test against. When a rule is triggered, an offense is created. You can assign the offense for investigation and remediation.

Data selection

The profile uses a saved search to collect the historical event and flow data to use in the run. Ensure that your security profile grants permission to view the events and flows that you want to include in the historical correlation run.

Rule selection and handling

The QRadar console processes data against only the rules that are specified in the historical correlation profile.

© Copyright IBM Corp. 2012, 2021

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

You can include disabled rules in a historical correlation profile. When the profile runs, the disabled rule is evaluated against the incoming events and flows. If the rule is triggered, and the rule action is to generate an offense, the offense is created even when the rule is disabled. To avoid generating unnecessary distractions, rule responses, such as report generation and mail notifications, are ignored during historical correlation.

Because historical correlation processing occurs in a single location, the rules that are included in the profile are treated as global rules. The processing does not change the rule from local to global, but handles the rule as if it were global during the historical correlation run. Some rules, such as stateful rules, might not trigger the same response as they would in a normal correlation that is run on a local event processor. For example, a local stateful rule that tracks five failed logins in 5 minutes from the same user name behaves differently under normal and historical correlation runs. Under normal correlation, this local rule maintains a counter for the number of failed logins that are received by each local event processor. In historical correlation, this rule maintains a single counter for the entire QRadar system. In this situation, offenses might be created differently compared to a normal correlation run.

Offense creation

Historical correlation runs create offenses only when a rule is triggered and the rule action specifies that an offense must be created. A historical correlation run does not contribute to a real-time offense, nor does it contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

The maximum number of offenses that can be created by a historical correlation run is 100. The historical correlation run stops when the limit is reached.

You can view historical offenses on the **Threat and Security Monitoring** dashboard and on the **Offenses** tab at the same time that you review real-time offenses.

Creating a historical correlation profile

You create a historical correlation profile to rerun past events and flows through the custom rules engine (CRE). The profile includes information about the data set and the rules to use during the run.

Restriction: You can create historical profiles only in IBM QRadar SIEM. You cannot create historical profiles in IBM QRadar Log Manager.

Before you begin

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

About this task

You can configure a profile to correlate by either start time or device time. *Start time* is the time when the events arrive at the event collector. *Device time* is the time that the event occurred on the device. Events can be correlated by start time or device time. Flows can be correlated by start time only.

You can include disabled rules in the profile. Rules that are disabled are indicated in the rules list with **(Disabled)** after the rule name.

A historical correlation run does not contribute to a real-time offense. It also does not contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

Attention: Historical correlation is a single threaded process and can take significantly longer to correlate the data than real-time analysis of the same data set. To reduce the processing time, be specific when you choose the historical data to analyze and the rule set to test against. If possible, avoid correlating all events against all rules.

If you create too many historical correlation profiles that have many rules that are assigned to them, your offenses can be slow to load. If your offenses are slow to load, you can either delete unneeded profiles or edit them to have fewer rules.

Procedure

1. Open the Historical Correlation dialog box.
   - On the **Log Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Network Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Click **Add** and select **Event Profile** or **Flow Profile**.
3. Type a name for the profile and select a saved search.

   You can use only nonaggregated saved searches.
4. On the **Rules** tab, select the rules to be run against the historical data, and choose the correlation time.

   If you select the **Use all enabled rules** checkbox, you cannot include disabled rules in the profile. If you want to include both enabled and disabled rules in the profile, you must select them individually from the rules list and click **Add Selected**.
5. On the **Schedule** tab, enter the time range for the saved search and set the profile schedule settings.
6. On the **Summary** tab, review the configuration and choose whether to run the profile immediately.
7. Click **Save**.

   The profile is put into a queue to be processed. Queued profiles that are based on a schedule take priority over manual runs.

Viewing information about historical correlation runs

View the history of a historical correlation profile to see information about past runs for the profile.

You can see the list of offenses that were created during the run and the catalog of events or flows that match the triggered rules in the profile. You can view the history for historical correlation runs that are queued, running, complete, complete with errors, and canceled.

About this task

For each rule in the profile that contributes to an offense, a catalog is created for each unique value of the property that the offense is indexed on. For each rule that does not contribute to an offense, a single catalog is created.

The following table shows how a historical correlation profile handles catalog creation under different scenarios. In each scenario, the catalog contains all the events or flows that either fully or partially match the triggered rule.

Table 42. Historical correlation catalog examples

Scenario	Result
A rule generates offenses that are indexed on source IP address. The events that triggered the rule have three different source IP addresses.	The historical correlation profile creates three catalogs.
A rule generates offenses that are indexed on username. The events that triggered the rule have five different usernames.	The historical correlation profile creates five catalogs.

Table 42. Historical correlation catalog examples (continued)

Scenario	Result
A rule is triggered, but the rule action does not create an offense.	The historical correlation profile creates a single catalog that includes all events that triggered the rule.

You cannot build reports on historical correlation data directly from QRadar. If you want to use third-party programs to build reports, you can export the data from QRadar.

Procedure

1. Open the **Historical Correlation** dialog box.
   - On the **Log Activity** or **Network Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Select a profile and click **View History**.
   a) If the historical correlation run status is **Completed** and the **Offense Count** is 0, the profile rules did not trigger any offenses.
   b) If the historical correlation run created offenses, in the **Offense Count** column, click the link to see a list of the offenses that were created.

If only one offense was created, the offense summary is shown.

3. In the **Catalogs** column, click the links to see the list of events that either fully or partially match the profile rules.

   The **StartTime** column in the event list represents the time that QRadar received the event.

4. Click **Close**.

Chapter 14. IBM X-Force integration

IBM X-Force security experts use a series of international data centers to collect tens of thousands of malware samples, to analyze web pages and URLs, and to run analysis to categorize potentially malicious IP addresses and URLs. You can use this data to identify and remediate undesirable activity in your environment before it threatens the stability of your network.

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

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

IBM Security Threat Content application

The **IBM Security Threat Content** application on the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) contains rules, building blocks, and custom properties that are intended for use with the X-Force.

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

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

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

Your QRadar administrator must install the **IBM Security Threat Content** application in order for the rules to appear in the **Threats** group in the **Rules List** window. The rules must be enabled before you can use them.

Enabling X-Force rules in IBM QRadar

By adding the IBM Security Threat Content application to your QRadar system, X-Force rules are added to the **Rules List**. The rules must be enabled before you can use them.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules** > **Rules**.
3. From the **Group** menu, click **Threats**.

   The **Group** column might show both legacy and enhanced rules. By default, X-Force legacy rules are disabled. However, you might see legacy rules that are enabled. Use the newer enhanced rules in the **Threat** group, and not the legacy rules that use the remote nets.

4. Select the **X-Force** rules in the **Threat** group and click **Actions** > **Enable/Disable**.

IP address and URL categories

X-Force Threat Intelligence categorizes IP address and URL information.

The IP addresses are grouped into the following categories:

© Copyright IBM Corp. 2012, 2021

- Malware hosts
- Spam sources
- Dynamic IP addresses
- Anonymous proxies
- Botnet Command and Control
- Scanning IP addresses

The X-Force Threat Intelligence feed also categorizes URL addresses. For example, URL addresses might be categorized as dating, gambling, or pornography sites. To see the complete list of categories for URL classification, see the IBM X-Force Exchange website (https://exchange.xforce.ibmcloud.com/faq).

Finding IP address and URL information in X-Force Exchange

Use right-click menu options in IBM QRadar to find information about IP addresses and URLs that is found on IBM Security X-Force Exchange. You can use the information from your QRadar searches, offenses, and rules to research further or to add information about IP addresses or URLs to an X-Force Exchange collection.

About this task

You can contribute either public or private information to track data in collections when you research security issues.

A *collection* is a repository where you store the information that is found during an investigation. You can use a collection to save X-Force Exchange reports, comments, or any other content. An X-Force Exchange report contains both a version of the report from the time when it was saved, and a link to the current version of the report. The collection contains a section that has a wiki-style notepad where you can add comments that are relevant to the collection.

For more information about X-Force Exchange, see X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procedure

1. To look up an IP address in X-Force Exchange from QRadar, follow these steps:
   a) Select the **Log Activity** or the **Network Activity** tab.
   b) Right-click the IP address that you want to view in X-Force Exchange and select **More Options** > **Plugin Options** > **X-Force Exchange Lookup** to open the X-Force Exchange interface.
2. To look up a URL in X-Force Exchange from QRadar, follow these steps:
   a) Select either the **Offenses** tab, or the event details windows available on the **Offenses**.

b) Right-click the URL you want to look up in X-Force Exchange and select **Plugin Options > X-Force Exchange Lookup** to open the X-Force Exchange interface.

Creating a URL categorization rule to monitor access to certain types of websites

You can create a rule that sends an email notification if users of the internal network access URL addresses that are categorized as gambling websites.

Before you begin

To use X-Force data in rules, your administrator must configure QRadar to load data from the X-Force servers.

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

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Actions** list, select **New Event Rule**.
4. Read the introductory text on the Rule wizard and click **Next**.
5. Click **Events** and click **Next**.
6. From the **Test Group** list box, select **X-Force Tests**.
7. Click the plus (+) sign beside the **when URL (custom) is categorized by X-Force as one of the following categories** test.
8. In the **enter rule name here** field in the Rule pane, type a unique name that you want to assign to this rule.
9. From the list box, select **Local** or **Global**.
10. Click the underlined configurable parameters to customize the variables of the test. a) Click **URL (custom)**.
    b) Select the URL property that contains the URL that was extracted from the payload and click**Submit**.
    c) Click **one of the following categories**.
    d) Select **Gambling / Lottery** from the X-Force URL categories, click **Add +** and click **Submit**.
11. 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**.
12. On the Groups pane, select the check boxes of the groups to which you want to assign this rule.
13. In the **Notes** field, type a note that you want to include for this rule, and click **Next**.
14. On the **Rule Responses** page, click **Email** and type the email addresses that receive the notification.
15. Click **Next**.
16. If the rule is accurate, click **Finish**.

Confidence factor and IP address reputation

IP address reputation data is evaluated on the time that it is seen and the volume of messages or data. X-Force categorizes IP address reputation data and assigns a confidence factor value 0 - 100, where 0

represents no confidence and 100 represents certainty. For example, X-Force might categorize a source IP address as a scanning IP with a confidence factor of 75, which is a moderately high level of confidence.

Determining a threshold

As an example, spam messages with an IP address reputation entry of 0 indicates that the source IP traffic is not spam, whereas an entry of 100 indicates definite spam traffic. Thus, values less than 50 indicate less probability that the message is spam, and values greater than 50 indicate more probability that the message is spam. A value of 50 or higher is the threshold where you might consider action on a triggered rule.

These probabilities are based on ongoing web-based data that IBM Security X-Force Threat Intelligence continuously collects and analyzes from around the world in X-Force data centers. As data is collected, the system evaluates how much spam is received from a particular IP address, or how frequently the flagged IP address is in the IP address reputation category. The more times, the higher the system scores the confidence factor.

Tuning false positives with the confidence factor setting

Use the confidence factor to limit the number of offenses that are created by triggered rules. Depending on the level of protection that you want, you adjust the confidence values to a level that best matches your network environment.

About this task

When you tune rules, consider a scale where 50 is the tipping point. On assets of lower importance, you might weigh an X-Force rule to trigger at a higher confidence factor for specific categories, like spam. For example, tuning a rule to a confidence factor of 75 means the rule triggers only when X-Force sees an IP address at or above a confidence factor of 75. This tuning reduces the number of offenses that are generated on lower priority systems and non-critical assets. However, an important system or critical business asset with a confidence factor of 50 triggers an offense at a lower level and brings attention to an issue more quickly.

For your DMZ, choose a higher confidence value such as 95% or higher. You do not need to investigate many offenses in this area. With a high confidence level, the IP addresses are more likely to match the category that is listed. If it is 95% certain that a host is serving malware, then you need to know about it.

For more secure areas of the network, like a server pool, lower the confidence value. More potential threats are identified and you spend less effort investigating because the threat pertains to a specific network segment.

For optimum false positive tuning, manage your rule triggers by segment. Look at your network infrastructure and decide which assets need a high level of protection, and which assets do not. You can apply different confidence values for the different network segments. Use building blocks for grouping commonly used tests so that they can be used in rules.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules** > **Rules**.

3. Double-click a rule to start the Rule wizard.
4. In the filter box, type the following text:

   when this host property is categorized by X-Force as this category with confidence value equal to this amount
5. Click the **Add test to rule (+)** icon.
6. In the Rule section, click the this amount link.
7. Enter a confidence value.
8. Click **Submit**.
9. Click **Finish** to exit the Rules wizard.

Searching data from IBM X-Force Exchange with advanced search criteria

For complex queries, you can search and filter data from X-Force Exchange by using Advanced Search expressions.

About this task

Advanced searches return data from the **Log Activity** or the **Network Activity** tab in QRadar.

URL searches cannot be returned from the **Network Activity** tab because the URL information is provided by the event data.

Procedure

1. Click the **Log Activity** tab.
2. On the **Search** toolbar, select the **Advanced Search**.
3. Type an AQL query expression.

   The following table describes some common search expressions.

Table 43. X-Force advanced search expressions

Description	Example
Searches for HTTP hosts from flows that match a bad category.	`select * from flows where XFORCE_URL_CATEGORY("HTTP Host") in ('Anonymization Services','Malware', 'Botnet Command and Control Server', 'Spam URLs', 'Cryptocurrency Mining', 'Bots', 'Phishing URLs')`
Searches for URLs found in events that match a bad category.	`select * from events where XFORCE_URL_CATEGORY("UrlHost") in ('Anonymization Services','Malware', 'Botnet Command and Control Server', 'Spam URLs', 'Cryptocurrency Mining', 'Bots', 'Phishing URLs')`

Searches for IP addresses that match a bad category with a confidence factor above 75.	select * from events where XFORCE_IP_CONFIDENCE('Anonymization Services',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Malware',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Botnet Command and Control Server',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Spam',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Cryptocurrency Mining',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Scanning IPs',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Bots',destinationaddress) > 75 OR XFORCE_IP_CONFIDENCE('Anonymization Services',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Malware',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Botnet Command and Control Server',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Spam',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Cryptocurrency Mining',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Scanning IPs',sourceaddress) > 75 OR XFORCE_IP_CONFIDENCE('Bots',sourceaddress) > 75
Searches associated with a URL.	select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL
Searches associated with a source IP address.	select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(destinationip) in ('Malware', 'Botnet Command and Control Server', 'Spam', 'Cryptocurrency Mining', 'Scanning IPs', 'Bots', 'Phishing')

4. Click **Search**.

Chapter 15. 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.

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 Graph types.

Chart types

When you create a report, you must choose a chart type for each chart you include in your report.

The chart type determines how the data and network objects appear in your report.

You can use any of the following types of charts:

© Copyright IBM Corp. 2012, 2021

Table 44. Chart Types

Chart Type	**Description**
None	Use this option if you need 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 QRadar Vulnerability Manager.
Connections	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Device Rules	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Device Unused Objects	This chart option is only displayed if you purchased and licensed IBM QRadar Risk Manager. For more information, see the *IBM QRadar Risk Manager User Guide*.
Events/Logs	Use this chart to view event information. You can base a chart on data from saved searches on the **Log Activity** tab. You can configure the chart to plot data over a configurable period of time to detect event trends. For more information about saved searches, see Chapter 10, “Event and flow searches,” on page 139.

Log Sources	Use this chart to export or report on log sources. Select the log sources and log source groups that you want to appear in the report. Sort log sources by report columns. Include log sources that are not reported for a defined time period. Include log sources that were created in a specified time period.
Flows	Use this chart to view flow information. You can base a chart on data from saved searches on the **Network Activity** tab. You can configure the chart to plot flow data over a configurable period of time to detect flow trends. For more information about saved searches, see Chapter 10, "Event and flow searches," on page 139.
Top Destination IPs	Use this chart to display the top destination IPs in the network locations you select.
Top Offenses	Use this chart to display the top offenses that occur at present time for the network locations you select.

Table 44. Chart Types (continued)	
Chart Type	**Description**
Offenses Over Time	Use this chart to display all offenses that have a start time within a defined time span for the network locations you select.
Top Source IPs	Use this chart to display and sort the top offense sources (IP addresses) that attack your network or business assets.
Vulnerabilities	The Vulnerabilities option is only displayed when the IBM QRadar Vulnerability Manager was purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

Table 45. Chart Types	
Chart Type	**Description**
None	Use this option if you need 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 QRadar Vulnerability Manager.
Vulnerabilities	The Vulnerabilities option is only displayed when the IBM QRadar Vulnerability Manager was purchased and licensed. For more information, see the *IBM QRadar Vulnerability Manager User Guide*.

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 46. Report toolbar options	
Option	**Description**
Group	

Manage Groups	Click **Manage Groups** to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups. You can share report groups with other users.

Table 46. Report toolbar options (continued)

Option	**Description**
Actions	Click **Actions** to perform the following actions: • **Create** - Select this option to create a new report. • **Edit** - Select this option to edit the selected report. You can also double-click a report to edit the content. • **Duplicate** - Select this option to duplicate or rename the selected report. • **Assign Groups** - Select this option to assign the selected report to a report group. • **Share** - Select this option to share the selected report with other users. You must have administrative privileges to share reports. • **Toggle Scheduling** - Select this option to toggle the selected report to the Active or Inactive state. • **Run Report** - Select this option to generate the selected report. To generate multiple reports, hold the Control key and click on the reports you want to generate. • **Run Report on Raw Data** - Select this option to generate the selected report using raw data. This option is useful when you want to generate a report before the required accumulated data is available. For example, if you want to run a weekly report before a full week has elapsed since you created the report, you can generate the report using this option. • **Delete Report** - Select this option to delete the selected report. To delete multiple reports, hold the Control key and click on the reports you want to delete. • **Delete Generated Content** - Select this option to delete all generated content for the selected rows. To delete multiple generated reports, hold the Control key and click on the generate reports you want to delete.

Hide Interactive Reports	Select this check box to hide inactive report templates. The **Reports** tab automatically refreshes and displays only active reports. Clear the check box to show the hidden inactive reports.

Table 46. Report toolbar options (continued)

Option	**Description**
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

Graph types

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

The network configuration files determine the colors that the charts use to depict network traffic. Each IP address is depicted by using a unique color. The following table provides examples of how network and security data is used in charts. The table describes the chart types that are available for each type of graph.

Table 47. Graph types

Graph type	**Available chart types**
Line	• Events/Logs • Flows • Connections • Vulnerabilities
Stacked Line	• Events/Logs • Flows • Connections • Vulnerabilities
Bar	• Events/Logs • Flows • Asset Vulnerabilities Connections • Connections • Vulnerabilities

Horizontal Bar	• Top Source IPs • Top Offenses • Offenses Over Time • Top Destination IPs
Stacked Bar	• Events/Logs • Flows • Connections

Table 47. Graph types (continued)

Graph type	**Available chart types**
Pie	• Events/Logs • Flows • Asset Vulnerabilities • Connections • Vulnerabilities
Table	• Events/Logs • Flows • Top Source IPs • Top Offenses • Offenses Over Time • Top Destination IPs • Connections • Vulnerabilities To display content in a table, you must design the report with a full page width container.
Aggregate Table	Available with the Asset Vulnerabilities chart. To display content in a table, you must design the report with a full page width container.

The following graph types are available for QRadar Log Manager reports:

- Line
- Stacked Line
- Bar
- Stacked Bar
- Pie
- Table

Note: When you create bar and stacked bar graph reports, the legend is presented in a fixed format and the bars or bar sections are represented by color coded labels in most cases. If you select time as the value for the x axis, you can create time intervals on the x axis.

Creating custom reports

Use the Report wizard to create and customize 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 QRadar 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 you create a report that generates weekly or monthly, the scheduled time must elapse 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 will return results after 7 days.

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 use 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!** window, click **Next**.
4. Select one of the following options:

Option	Description
Manually	By default, the report generates 1 time. You can generate the report as often as you want.
Hourly	Schedules the report to generate at the end of each hour. The data from the previous hour is used. From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m for both the **From** and **To** fields.
Daily	Schedules the report to generate at the end of each day. The data from the previous day is used. From the list boxes, select the time and the days of the week that you want the report to run.

Weekly	Schedules the report to generate weekly using the data from the previous calendar week, from Monday to Sunday. 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.
Monthly	Schedules the report to generate monthly using the data from the previous calendar month. From the list box, select the date that you want to generate the report. The default is the first day of the month. Select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

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 **Portrait** or **Landscape** for the page orientation.
   b) Select one of the six layout options that are displayed on the Report wizard.c) Click **Next** .
7. Specify values for the following parameters:

Parameter	Values
Report Title	The title can be up to 60 characters in length. Do not use special characters.
Logo	From the list box, select a logo.
Pagination Options	From the list box, select a location for page numbers to display on the report. You can choose not to have page numbers display.
Report Classification	Type a classification for this report. You can type up to 75 characters in length. You can use leading spaces, special characters, and double byte characters. The report classification displays in the header and footer of the report. You might want to classify your report as confidential, highly confidential, sensitive, or internal.

8. Configure each container in the report:
   a) From the **Chart Type** list box, select a chart type.
   b) On the **Container Details** window, configure the chart parameters.

      Note: You can also create asset saved searches. From the **Search to use** list box, select your saved search.

   c) Click **Save Container Details**.
   d) If you selected more than one container, repeat steps a to c.
   e) Click **Next** .
9. Preview the **Layout Preview** page, and then click **Next**.
10. Select the check boxes for the report formats you want to generate, and then click **Next**.

    Important: 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:

Option	Description

Report Console	Select this check box to send the generated report to the **Reports** tab. **Report Console** is the default distribution channel.
Select the users that should be able to view the generated report.	This option displays after you select the **Report Console** check box. From the list of users, select the users that you want to grant permission to view the generated reports.
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all users to view the generated reports. You must have appropriate network permissions to share the generated report with other users.
Email	Select this check box if you want to distribute the generated report by email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter are 255. Email recipients receive this email from no_reply_reports@qradar.
Include Report as attachment (nonHTML only)	This option is only displayed after you select the **Email** check box. Select this check box to send the generated report as an attachment.
Option	**Description**
Include link to Report Console	This option is only displayed after you select the **Email** check box. Select this check box to include a link to the Report Console in the email.

12. On the **Finishing Up** page, enter values for the following parameters.

Option	Description
Report Description	Type a description for this report. The description is displayed on the **Report Summary** page and in the generated report distribution email.
Please select any groups you would like this report to be a member of	Select the groups to which you want to assign this report. For more information about groups, see Report groups.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

13. Click **Next** to view the report summary.
14. On the **Report Summary** page, select the tabs available on the summary report to preview your report configuration.

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.

Related information

Creating reports in QRadar SIEM

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.

Note: When you customize a scheduled report to generate manually, select the time span **End Date** before you select the **Start Date**.

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 yourequire.

Results

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.

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, 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.

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 **Report**s 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
- VoIP
- Other

When you create a new report, you can assign the report to an existing group or create a new group. You must have administrative access to create, edit, or delete groups.

For more information about user roles, see the *IBM QRadar 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.
4. Click **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 onthe navigation tree.
8. Close the **Report Groups** window.

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**.
7. Close the **Report Groups** window.

Sharing report groups

You can share report groups with other users.

Before you begin

You must have administrative permissions to share a report group with other users.

For more information about permissions, see the *IBM QRadar Administration Guide*.

You cannot use the Content Management Tool (CMT) to share report groups.

For more information about the CMT, see the *IBM QRadar Administration Guide*

About this task

On the **Report Groups** window, shared users can see the report group in the report list.

To view a generated report, the user must have permission to view the report.

Procedure

1. Click the **Reports** tab.
2. On the **Reports** window, click **Manage Groups**.
3. On the **Report Groups** window, select the report group that you want to share and click **Share**.
4. On the **Sharing Options** window, select one of the following options.

Option	Description
Default (inherit from parent)	The report group is not shared. Any copied report group or generated report remains in the users report list.
Option	**Description**
	Each report in the group is assigned any parent report sharing option that was configured.

Share with Everyone	The report group is shared with all users.
Share with users matching the following criteria...	The report group is shared with specific users. **User Roles** Select from the list of user roles and press the add icon (+). **Security Profiles** Select from the list of security profiles and press the add icon (+).

5. Click **Save**.

Results

On the **Report Groups** window, shared users see the report group in the report list. Generated reports display content based on security profile setting.

Related tasks

"Creating custom reports" on page 218

Use the Report wizard to create and customize a new report.

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**.
7. Close the **Report Groups** window.

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**.
7. Close the **Report Groups** window.