IBM Security QRadar SIEM Administration Guide

Version 7.2.1

Administration Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 251.

Contents

About this guide

The IBM Security QRadar SIEM Administration Guide provides information on managing IBM Security QRadar SIEM including the Dashboard, Offenses, Log Activity, Network Activity, Assets, and Reports tabs.

Intended audience

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

Technical documentation

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

Contacting customer support

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

Statement of good security practices

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

Chapter 1. Overview

General information on how to access and use the IBM Security QRadar® user interface and the **Admin** tab

This overview includes general information on how to access and use the user interface and the **Admin** tab.

Supported web browsers

You access the IBM Security QRadar console from a standard web browser.

When you access the system, a prompt is displayed asking for a user name and a password. The user name and password must be configured in advance by the administrator.

Table 1. Supported web browsers

Web browser	Supported version
Mozilla Firefox	• 10.0 ESR • 17.0 ESR Mozilla Firefox has a short release cycle. We cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.
Microsoft Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0
Google Chrome	• Latest version We are fully committed to investigating any issues that are reported.

Admin tab overview

The **Admin** tab provides several tab and menu options that allow you to configure QRadar.

You must have administrative privileges to access administrative functions. To access administrative functions, click the **Admin** tab on the user interface.

The **Admin** tab provides access to the following functions:

- Manage users. See Chapter 2, “User management,” on page 7.
- Manage your network settings. See Chapter 3, “Managing the system and licenses,” on page 25.
- Manage high availability. See the *IBM Security QRadar High Availability Guide*.
- Manage QRadar SIEM settings. See Chapter 5, “Set up QRadar SIEM,” on page 53.
- Manage references sets. See Chapter 6, “Reference sets management,” on page 87.

- Manage authorized services. See Chapter 8, “Managing authorized services,” on page 99.
- Backup and recover your data. See Chapter 9, “Manage backup and recovery,” on page 103.
- Manage your deployment views. See Chapter 10, “Deployment editor,” on page 115.
- Manage flow sources. See Chapter 11, “Flow sources management,” on page 145.
- Configure remote networks and remote services. See Chapter 12, “Remote networks and services configuration,” on page 153.
- Discover servers. See Chapter 13, “Server discovery,” on page 157.
- Configure data forwarding. See Chapter 14, “Data forwarding,” on page 159.
- Managing vulnerability scanners. For more information, see the *Managing Vulnerability Assessment Guide*.
- Configure plug-ins. For more information, see the associated documentation.
- Configure the IBM Security QRadar Risk Manager. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.
- Manage log sources. For more information, see the *IBM Security QRadar Log Sources Users Guide*.

The **Admin** tab also includes the following menu options:

Table 2. Admin tab menu options

Menu option	Description
Deployment Editor	Opens the Deployment Editor window. For more information, see Chapter 10, “Deployment editor,” on page 115.
Deploy Changes	Deploys any configuration changes from the current session to your deployment. For more information, see “Deploying changes.”
Advanced	The **Advanced** menu provides the following options: **Clean SIM Model** - Resets the SIM module. See “Resetting SIM” on page 4. **Deploy Full Configuration** - Deploys all configuration changes. For more information, see “Deploying changes.”

Deploying changes

You can update your configuration settings from the **Admin** tab. Your changes are saved to a staging area where they are stored until you manually deploy the changes.

About this task

Each time that you access the **Admin** tab and each time you close a window on the **Admin** tab, a banner at the top of the **Admin** tab displays the following message: `Checking for undeployed changes`.If undeployed changes are found, the banner updates to provide information about the undeployed changes.

If the list of undeployed changes is lengthy, a scroll bar is provided. Scroll through the list.

The banner message also suggests which type of deployment change to make. Choose one of the two options:

- **Deploy Changes** - Click the **Deploy Changes** icon on the **Admin** tab toolbar to deploy any configuration changes from the current session to your deployment.
- **Deploy Full Configuration** - Select **Advanced** > **Deploy Full Configuration** from the **Admin** tab menu to deploy all configuration settings to your deployment. All deployed changes are then applied throughout your deployment.

  Important: When you click **Deploy Full Configuration**, QRadar SIEM restarts all services, which result in a gap in data collection until deployment completes.

After you deploy your changes, the banner clears the list of undeployed changes and checks the staging area again for any new un`deployed changes. If none are present, the following message is displayed: `There are no changes to deploy.`

Procedure

1. Click **View Details**
2. Choose one of the following options:
   a. To expand a group to display all items, click the plus sign (+) beside the text. When done, you can click the minus sign (-).
   b. To expand all groups, click **Expand All**. When done, you can click **Collapse All**.
   c. Click **Hide Details** to hide the details from view again.
3. Perform the suggested task:
   a. From the **Admin** tab menu, click **Deploy Changes**.
   b. From the **Admin** tab menu, click **Advanced** > **Deploy Full Configuration**.

Updating user details

You can access your administrative user details through the main user interface.

Procedure

1. Click **Preferences**
2. Optional. Update the configurable user details:

Option	Description
Parameter	Description
Email	Type a new email address
Password	Type a new password
Password (Confirm)	Type the new password again
Enable Popup Notifications	Popup system notifications are displayed at the lower right corner of the user interface. To disable popup notifications, clear this check box. For more information about popup notifications, see the *Users Guide* for your product.

3. Click **Save**.

Resetting SIM

Use the **Admin** to reset the SIM module. This allows you to remove all offense, source IP address, and destination IP address information from the database and the disk.

About this task

This option is useful after you tune your deployment to avoid receiving any additional false positive information.

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

Procedure

1. Click the **Admin** tab.
2. From the **Advanced** menu, select **Clean SIM Model**.
3. Read the information on the Reset SIM Data Module window.
4. Select one of the following options.

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

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

Monitoring systems with SNMP

This topic provides information about the monitoring of appliances through SNMP polling.

QRadar SIEM uses the Net-SNMP agent, which supports various system resource monitoring MIBs. They can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information about Net-SNMP, see Net-SNMP documentation.

Managing aggregated data views

A large volume of data aggregation can decrease system performance. To improve system performance, you can disable, enable, or delete aggregated data views. Time series charts, report charts, and anomaly rules use aggregated data views.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Aggregated Data Management** icon.
4. To filter the list of aggregated data views, choose an option from one the following options:
   - Select an option from one of the following lists: **View**, **Database**, **Show**, or **Display**.
   - Type an aggregated data ID, report name, chart name, or saved search name in the search field.
5. To manage an aggregated data view, select the view, and then the appropriate action from the toolbar:
   - If you select **Disable View** or **Delete View**, a window displays content dependencies for the aggregated data view. After you disable or delete the aggregated data view, the dependent components no longer use aggregated data.
   - If you enable a disabled aggregated data view, the aggregated data from the deleted view is restored.

Chapter 2. User management

Provides information and procedures for configuring and managing user accounts.

When you initially configure QRadar SIEM, you must create user accounts for all users that require access to QRadar SIEM. After initial configuration, you can edit user accounts to ensure that user information is current. You can also add and delete user accounts as required.

User management overview

A user account defines the user name, default password, and email address for a user.

Assign the following items for each new user account you create:

- **User role** - Determines the privileges that the user is granted to access functions and information in QRadar SIEM. QRadar SIEM includes two default user roles: Admin and All. Before you add user accounts, you must create more user roles to meet the specific permissions requirement of your users.
- **Security profile** - Determines the networks and log sources the user is granted access to. QRadar SIEM includes one default security profile for administrative users. The Admin security profile includes access to all networks and log sources. Before you add user accounts, you must create more security profiles to meet the specific access requirements of your users.

Role management

Using the User Roles window, you can create and manage user roles.

Using the User Roles window, you can create and manage user roles.

Creating a user role

Use this task to create the user roles that are required for your deployment.

About this task

By default, your system provides a default administrative user role, which provides access to all areas of QRadar SIEM. Users who are assigned an administrative user role cannot edit their own account. This restriction applies to the default Admin user role. Another administrative user must make any account changes.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **User Roles** icon.
4. On the toolbar, click **New**.
5. Configure the following parameters:
   a. In the **User Role Name** field, type a unique name for this user role.

b. Select the permissions that you want to assign to this user role. See "User role parameters" on page 19.

6. Click **Save**.
7. Close the User Role Management window.
8. On the **Admin** tab menu, click **Deploy Changes**.

Editing a user role

You can edit an existing role to change the permissions that are assigned to the role.

About this task

To quickly locate the user role you want to edit on the User Role Management window, you can type a role name in the **Type to filter** text box. This box is located above the left pane.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **User Roles** icon.
4. In the left pane of the User Role Management window, select the user role that you want to edit.
5. On the right pane, update the permissions, as necessary. See "User role parameters" on page 19.
6. Click **Save**.
7. Close the User Role Management window.
8. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a user role

If a user role is no longer required, you can delete the user role.

About this task

If user accounts are assigned to the user role you want to delete, you must reassign the user accounts to another user role. The system automatically detects this condition and prompts you to update the user accounts.

You can quickly locate the user role that you want to delete on the User Role Management window. Type a role name in the **Type to filter** text box, which is located above the left pane.

Procedure

1. Click the **Admin** tab.
2. On the**Navigation** menu, click **System Configuration** > **User Management**.
3. Click the**User Roles** icon.
4. In the left pane of the User Role Management window, select the role that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.

- If user accounts are assigned to this user role, the Users are Assigned to this User Role window opens. Go to Step 7.
- If no user accounts are assigned to this role, the user role is successfully deleted. Go to Step 8.

7. Reassign the listed user accounts to another user role:
   a. From the **User Role to assign** list box, select a user role.
   b. Click **Confirm**.
8. Close the User Role Management window.
9. On the **Admin** tab menu, click **Deploy Changes**.

Managing security profiles

Security profiles define which networks and log sources a user can access and the permission precedence.

Using theSecurity Profile Management window, you can view, create, update, and delete security profiles.

Permission precedences

This topic defines each of the permission precedence options.

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

Make sure that you understand the following restrictions:

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

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

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

For example, if an event is associated with a log source the security profile allows access to, but the destination network is restricted, the event is displayed in the **Log Activity** tab. The event must match one requirement.

Creating a security profile

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

About this task

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

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

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

Procedure

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

Editing a security profile

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

About this task

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

Procedure

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

Option	Description
Keep Old Data and Save	Select this option to keep previously accumulated time series data. If you choose this option, issues might occur when users associated with this security profile views time series charts.
Hide Old Data and Save	Select this option to hide the time-series data. If you choose this option, time series data accumulation restarts after you deploy your configuration changes.

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

Duplicating a security profile

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

About this task

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration User Management**.
3. Click the **Security Profiles** icon.
4. In the left pane, select the security profile you want to duplicate.
5. On the toolbar, click **Duplicate** .
6. In the Confirmation window, type a unique name for the duplicated security profile.
7. Click **OK** .

8. Update the parameters as required.
9. Close the Security Profile Management window.
10. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a security profile

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

About this task

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

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Security Profiles** icon.
4. In the left pane, select the security profile that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.
   - If user accounts are assigned to this security profile, the Users are Assigned to this Security Profile window opens. Go to "Deleting a user role" on page 8.
   - If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to "Deleting a user role" on page 8.
7. Reassign the listed user accounts to another security profile:
   a. From the **User Security Profile to assign** list box, select a security profile.
   b. Click **Confirm**.
8. Close the Security Profile Managementwindow.
9. On the **Admin** tab menu, click **Deploy Changes**.

User account management

This topic provides information about managing user accounts.

When you initially configure your system, you must create user accounts for each of your users. After initial configuration, you might be required to create more user accounts and manage existing user accounts.

Creating a user account

You can create new user accounts.

Before you begin

Before you can create a user account, you must ensure that the required user role and security profile are created.

About this task

When you create a new user account, you must assign access credentials, a user role, and a security profile to the user. User Roles define what actions the user has permission to perform. Security Profiles define what data the user has permission to access.

You can create multiple user accounts that include administrative privileges; however, any Administrator Manager user accounts can create other administrative user accounts.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Users** icon.
4. On the **User Management** toolbar, click **New**.
5. Enter values for the following parameters:
   a. In the **Username** field, type a unique user name for the new user. The user name must contain a maximum 30 characters.
   b. In the **Password** field, type a password for the user to gain access.
      The password must meet the following criteria:
      - Minimum of 5 characters
      - Maximum of 255 characters
6. Click **Save**.
7. Close the User Details window.
8. Close the User Management window.
9. On the **Admin** tab menu, click **Deploy Changes**.

Editing a user account

About this task

You can quickly locate the user account that you want to edit on the User Management window. Type the user name in the**Search User** text box, which is on the toolbar.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Users** icon.
4. On the User Management window, select the user account that you want to edit.
5. On the toolbar, click **Edit**.
6. Update parameters, as necessary. See “User Management window parameters” on page 23
7. Click **Save**.
8. Close the User Details window.
9. Close the User Management window.
10. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a user account

If a user account is no longer required, you can delete the user account.

About this task

After you delete a user, the user no longer has access to the user interface. If the user attempts to log in, a message is displayed to inform the user that the user name and password is no longer valid. Items that a deleted user created, such as saved searches and reports remain associated with the deleted user.

To quickly locate the user account you want to delete on the User Management window, you can type the user name in the **Search User** text box on the toolbar.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Users** icon.
4. Select the user that you want to delete.
5. On the toolbar, click **Delete**.
6. Click **OK**.
7. Close the User Management window.

Authentication management

This topic provides information and instructions for how to configure authentication.

QRadar SIEM supports various authentication types. You can configure authentication to validate users and passwords.

Authentication overview

When authentication is configured and a user enters an invalid user name and password combination, a message is displayed to indicate that the login was invalid.

If the user attempts to access the system multiple times with invalid information, the user must wait the configured amount of time before another attempt to access the system again. You can configure Console settings to determine the maximum number of failed logins, and other related settings. For more information about configuring Console settings for authentication, see Chapter 5, “Set up QRadar SIEM,” on page 53 “Configuring the Console settings” on page 79.

An administrative user can access QRadar SIEM through a vendor authentication module or by using the local Admin password. The Admin password functions if you set up and activated a vendor authentication module. However, you cannot change the Admin password while the authentication module is active. To change the Admin password, you must temporarily disable the vendor authentication module, reset the password, and then reconfigure the vendor authentication module.

QRadar SIEM supports the following user authentication types:

- **System authentication** - Users are authenticated locally. This is the default authentication type.

- **RADIUS authentication** - Users are authenticated by a Remote Authentication Dial-in User Service (RADIUS) server. When a user attempts to log in, QRadar SIEM encrypts the password only, and forwards the user name and password to the RADIUS server for authentication.
- **TACACS authentication** - Users are authenticated by a Terminal Access Controller Access Control System (TACACS) server. When a user attempts to log in, QRadar SIEM encrypts the user name and password, and forwards this information to the TACACS server for authentication. TACACS Authentication uses Cisco Secure ACS Express® as a TACACS server. QRadar SIEM supports up to Cisco Secure ACS Express 4.3.
- **Active directory** - Users are authenticated by a Lightweight Directory Access Protocol (LDAP) server that uses Kerberos.
- **LDAP** - Users are authenticated by a Native LDAP server.

Before you begin

Prerequisite to configuring RADIUS, TACACS, Active Directory, or LDAP as the authentication type.

Before you can configure RADIUS, TACACS, Active Directory, or LDAP as the authentication type, you must complete the following tasks:

- Configure the authentication server before you configure authentication in QRadar. For more information, see your server documentation
- Ensure that the server has the appropriate user accounts and privilege levels to communicate with QRadar. For more information, see your server documentation.
- Ensure that the time of the authentication server is synchronized with the time of the QRadar server. For more information about setting time, see Chapter 5, "Set up QRadar SIEM," on page 53.
- Ensure that all users have appropriate user accounts and roles to allow authentication with the vendor servers.

Configuring system authentication

You can configure local authentication on your QRadar system.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Authentication** icon.
4. From the **Authentication Module** list box, select the **System Authentication**.
5. Click **Save**.

Configuring RADIUS authentication

You can configure RADIUS authentication on your QRadar system.

Procedure

1. Click the **Admin** tab.
2. On the **navigation** menu, click **System Configuration User Management**.
3. Click the **Authentication** icon.
4. From the **Authentication Module** list box, select **RADIUS Authentication**.
5. Configure the parameters:

a. In the **RADIUS Server** field, type the host name or IP address of the RADIUS server.
b. In the **RADIUS Port** field, type the port of the RADIUS server.
c. From the **Authentication Type** list box, select the type of authentication you want to perform.

   Choose from the following options:

Option	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows workstations.
ARAP	Apple Remote Access Protocol (ARAP) establishes authentication for AppleTalk network traffic.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server.

d. In the **Shared Secret** field, type the shared secret that QRadar SIEM uses to encrypt RADIUS passwords for transmission to the RADIUS server.

6. Click **Save**.

Configuring TACACS authentication

You can configure TACACS authentication on your QRadar system.

Procedure

1. Click the **Admin** tab.
2. On the **navigation** menu, click **System Configuration** > **User Management**.
3. Click the **Authentication** icon.
4. From the **Authentication Module** list box, select **TACACS Authentication**.
5. Configure the parameters:
   a. In the **TACACS Server** field, type the host name or IP address of the TACACS server.
   b. In the **TACACS Port** field, type the port of the TACACS server.
   c. From the **Authentication Type** list box, select the type of authentication you want to perform.

      Choose from the following options::

Option	Description
ASCII	American Standard Code for Information Interchange (ASCII) sends the user name and password in clear, unencrypted text.
PAP	Password Authentication Protocol (PAP) sends clear text between the user and the server. This is the default authentication type.

Option	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) establishes a Point-to-Point Protocol (PPP) connection between the user and the server.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authenticates remote Windows workstations.
MSCHAP2	Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAP2) authenticates remote Windows workstations using mutual authentication.
EAPMD5	Extensible Authentication Protocol using MD5 Protocol (EAPMD5) uses MD5 to establish a PPP connection.

d. In the **Shared Secret** field, type the shared secret that QRadar SIEM uses to encrypt TACACS passwords for transmission to the TACACS server.

6. Click **Save**.

Configuring Active Directory authentication

You can configure Active Directory authentication on your IBM Security QRadar system.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management**.
3. Click the **Authentication** icon.
4. From the **Authentication Module** list box, select **Active Directory**.

   Configure the following parameters:

Parameter	Description
Server URL	Type the URL used to connect to the LDAP server. For example, ldaps://<host>:<port>. You can use a space-separated list to specify multiple LDAP servers.
LDAP Context	Type the LDAP context you want to use, for example, DC=QRADAR,DC=INC.
LDAP Domain	Type the LDAP context you want to use, for example, DC=QRADAR,DC=INC.
LDAP Domain	Type the domain that you want to use, for example qradar.inc.

5. Click **Save**.

Configuring LDAP authentication

You can configure LDAP authentication on your IBM Security QRadar system.

Before you begin

If you plan to enable the SSL or TLS connection to your LDAP server, you must import the SSL or TLS certificate from the LDAP server to the

/opt/qradar/conf/trusted_certificates directory on your Console system. For more information about configuring the SSL certificate, see "Configuring Your SSL or TLS certificate."

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration User Management**.
3. Click the **Authentication** icon.
4. From the **Authentication Module** list box, select **LDAP**. Configure the following parameters:

Parameter	Description
Server URL	Type the URL used to connect to the LDAP server. For example, ldaps://<host>:<port>. You can use a space-separated list to specify multiple LDAP servers.
SSL Connection	Select **True** to use Secure Socket Layer (SSL) encryption to connect to the LDAP server. If SSL encryption is enabled, the value in the **Server URL** field must specify a secure connection. For example, ldaps://secureldap.mydomain.com:636".
TLS Authentication	From the list box, select **True** to start Transport Layer Security (TLS) encryption to connect to the LDAP server. The default is True. TLS is negotiated as part of the normal LDAP protocol and does not require a special protocol designation or port in the **Server URL** field.
Search Entire Base	Select one of the following options: • True - Select to search all subdirectories of the specified Directory Name (DN). • False -Select to search the immediate contents of the Base DN. The subdirectories are not searched.
LDAP User Field	Type the user field identifier that you want to search on, for example, uid. You can use a comma-separated list to search for multiple user identifiers.
Base DN	Type the base DN for required to perform searches, for example, DC=IBM,DC=INC.

5. Click **Save**.

Configuring Your SSL or TLS certificate

If you use LDAP for user authentication and you want to enable SSL or TLS, you must configure your SSL or TLS certificate.

Procedure

1. Using SSH, log in to your system as the root user.
   a. User name: root

b. Password: <password>

2. Type the following command to create the /opt/qradar/conf/trusted_certificates/ directory:mkdir -p /opt/qradar/conf/trusted_certificates
3. Copy the SSL or TLS certificate from the LDAP server to the /opt/qradar/conf/trusted_certificates directory on your system.
4. Verify that the certificate file name extension is .cert, which indicates that the certificate is trusted. QRadar SIEM only loads .cert files.

User role parameters

Descriptions for the User Role Management window parameters

The following table provides descriptions for the User Role Management window parameters.

Table 3.

Parameter	Description
User Role Name	Type a unique name for the role. The user role name must meet the following requirements:
Admin	Select this check box to grant the user administrative access to the user interface. After you select the **Admin** check box, all permissions check boxes are selected by default. Within the Admin role, you can grant individual access to the following Admin permissions: • **Administrator Manager** - Select this check box to allow users to create and edit other administrative user accounts. If you select this check box, the **System Administrator** check box is automatically selected. • **Remote Networks and Services Configuration** - Select this check box to allow users to configure remote networks and services on the **Admin** tab. • **System Administrator** - Select this check box to allow users to access all areas of user interface. Users with this access are not able to edit other administrator accounts.

Table 3. (continued)

Parameter	Description
Offenses	Select this check box to grant the user access to all **Offenses** tab function. Within the Offenses role, you can grant individual access to the following permissions: • **Assign Offenses to Users** - Select this check box to allow users to assign offenses to other users. • **Maintain Custom Rules** - Select this check box to allow users to create and edit custom rules. If you select this check box, the **View Custom Rules** check box is automatically selected. • **Manage Offense Closing Reasons** - Select this check box to allow users to manage offense closing reasons. • **View Custom Rules** - Select this check box to allow this user role to view custom rules. This permission, when granted to a user role that does not also have the **Maintain Custom Rules** permission, allows the user role to view custom rules details. The user role is not able to create or edit custom rules. For more information about the **Offenses** tab, see the *Users Guide* for your product.
Log Activity	Select this check box to grant the user access to all **Log Activity** tab function. Within the Log Activity role, you can also grant users individual access to the following permissions: • **Maintain Custom Rules** - Select this check box to allow users to create or edit rules that usethe **Log Activity** tab. • **Manage Time Series** - Select this check box to allow users to configure and view time series data charts. • **User Defined Event Properties** - Select this check box to allow users to create custom event properties. For more information about custom event properties, see the *Users Guide* for your product. • **View Custom Rules** - Select this check box to allow this user role to view custom rules. This permission, when granted to a user role that does not also have the **Maintain Custom Rules** permission, allows the user role to view custom rules details. The user role is not able to create or edit custom rules. For more information about the **Log Activity** tab, see the *Users Guide* for your product.

Table 3. (continued)

Parameter	Description
Assets	**Note:** This permission is only displayed if IBM Security QRadar Vulnerability Manager is installed on your system. Select this check box to grant the user access to all **Assets** tab function. Within the Assets role, you can grant individual access to the following permissions: • **Perform VA Scans** - Select this check box to allow users to complete vulnerability assessment scans. For more information about vulnerability assessment, see the *Managing Vulnerability Assessment guide*. • **Remove Vulnerabilities** - Select this check box to allow users to remove vulnerabilities from assets. • **Server Discovery** - Select this check box to allow users to discover servers. • **View VA Data** - Select this check box to allow users access to vulnerability assessment data. For more information about vulnerability assessment, see the *Managing Vulnerability Assessment guide.*
Network Activity	Select this check box to grant the user access to all **Network Activity** tab function. Within the Network Activity role, you can grant individual access to the following permissions: • **Maintain Custom Rules** - Select this check box to allow users to create or edit rules from the **Network Activity** tab. • **Manage Time Series** - Select this check box to allow users to configure and view time series data charts. • **User Defined Flow Properties** - Select this check box to allow users to create custom flow properties. • **View Custom Rules** - Select this check box to allow this user role to view custom rules. This permission, when granted to a user role that does not also have the **Maintain Custom Rules** permission, allows the user role to view custom rules details. The user role is not able to create or edit custom rules. • **View Flow Content** - Select this check box to allow users access to flow data. For more information about the **Network Activity** tab, see the *Users Guide* for your product.

Table 3. (continued)

Parameter	Description
Reports	Select this check box to grant the user access to all **Reports** tab function. Within the Reports role, you can grant users individual access to the following permissions: • **Distribute Reports via Email** - Select this check box to allow users to distribute reports through email. • **Maintain Templates** - Select this check box to allow users to edit report templates. For more information, see the *Users Guide* for your product.
Vulnerability Manager	This option is only available if IBM Security QRadar Vulnerability Manager is activated. Select this check box to grant users access to QRadar Vulnerability Manager function. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.
IP Right Click Menu Extensions	Select this check box to grant the user access to options added to the right-click menu.
Risks	This option is only available if IBM Security QRadar Risk Manager is activated. Select this check box to grant users access to QRadar Risk Manager function. For more information, see the *IBM Security QRadar Risk Manager User Guide*.

Security profile parameters

The following table provides descriptions of the Security Profile Management window parameters:

Table 4. Security Profile Management window parameters

Parameter	Description
Security Profile Name	Type a unique name for the security profile. The security profile name must meet the following requirements: • Minimum of 3 characters • Maximum of 30 characters
Description	`Optional.` Type a description of the security profile. The maximum number of characters is 255.

User Management window parameters

The following table provides descriptions of User Management window parameters:

Table 5. User Management window parameters

Parameter	Description
Username	Displays the user name of this user account.
Description	Displays the description of the user account.
E-mail	Displays the email address of this user account.
User Role	Displays the user role that is assigned to this user account. User Roles define what actions the user has permission to perform.
Security Profile	Displays the security profile that is assigned to this user account. Security Profiles define what data the user has permission to access.

User management window toolbar

User management window toolbar functions

The following table provides descriptions of the User Management window toolbar functions:

Table 6. User Management window toolbar functions

Function	Description
New	Click this icon to create a user account. For more information about how to create a user account, see “Creating a user account” on page 12.
Edit	Click this icon to edit the selected user account. For more information about how to edit a user account, see “Editing a user account” on page 13.
Delete	Click this icon to delete the selected user account. For more information about how to delete a user account, see “Deleting a user account” on page 14.
Search Users	In this text box, you can type a keyword and then press Enter to locate a specific user account.

User Details window parameters

User Details window parameters

The following table provides descriptions of the User Details window parameters:

Table 7. User Details window parameters

Parameter	Description
Username	Type a unique user name for the new user. The user name must contain a maximum of 30 characters.
E-mail	Type the user's email address. The email address must meet the following requirements: • Must be a valid email address • Minimum of 10 characters • Maximum of 255 characters
Password	Type a password for the user to gain access. The password must meet the following criteria: • Minimum of 5 characters • Maximum of 255 characters
Confirm Password	Type the password again for confirmation.
Description	`Optional.` Type a description for the user account. The maximum number of characters is 2,048.
User Role	From the list box, select the user role that you want to assign to this user. To add, edit, or delete user roles, you can click the **Manage User Roles** link. For information on user roles, see "Role management" on page 7.
Security Profile	From the list box, select the security profile that you want to assign to this user. To add, edit, or delete security profiles, you can click the **Manage Security Profiles** link. For information on security profiles, see "Managing security profiles" on page 9.

Chapter 3. Managing the system and licenses

You can manage the licenses, HA, and systems in your deployment.

You must allocate a license for each system in your deployment, including software appliances.QFlow and Event Collectors do not require a license.

When you install a QRadar system, a default license key provides you with access to the user interface for five weeks. Before the default license expires, you must allocate a license key to your system. You can also add licenses to enable QRadar products, such as QRadar Vulnerability Manager.

There is a 14 day grace period to reallocate a license. You can unlock a license if the key is uploaded, after a host is patched with a fix, or after an unlock key is uploaded. After the grace period is passed, the license is locked to the system.

If your license status is **Invalid**, the license must be replaced. The status might indicate that your license has been altered without authorization.

A license remains undeployed until you deploy the license change.

System and License Management window overview

You can use the System and License Management window to manage your license keys, restart or shut down your system, and configure access settings.

The toolbar on the System and License Management window provides the following functions:

Table 8. System and License Management toolbar functions

Function	Description
Allocate License to System	Use this function to allocate a license to a system. When you select **Licenses** from the **Display** list box, the label on this function changes to **Allocate System to Licenses**. For more information, see “Allocating a system to a license” on page 35 or “Allocating a license to a system” on page 31.
Upload License	Use this function to upload a license to your Console. For more information, see “Uploading a license key” on page 31.

Table 8. System and License Management toolbar functions (continued)

Function	Description
Actions (License)	If you select **Licenses** from the **Display** list box in the Deployment Details pane, the following functions are available on the **Actions** menu: • **Revert Allocation** - Select this option to undo license changes. The action reverts the license to the previous state. If you select **Revert Allocation** on a deployed license within the allocation grace period, which is 14 days after deployment, the license state changes to **Unlocked** so that you can reallocate the license to another system. • **Delete License** - Select a license from the list, and then select this option to delete the license from your system. This option is not available for undeployed licenses. • **View License** - Select a license from the list, and then select this option to view the Current License Details window. • **Export Licenses** - Select this option to export the listed licenses to an external file that you can store on your desktop system. For more information, see "Exporting a license" on page 33.

Table 8. System and License Management toolbar functions (continued)

Function	Description
Actions (System)	If you select **Systems** from the **Display** list box in the Deployment Details pane, the following functions are available on the **Actions** menu: • **View System** - Select a system, and then select this option to view the System Details window. For more information, see "Viewing system details" on page 34. • **Revert Allocation** - Select this option to undo staged license changes. The configuration reverts to the last deployed license allocation. If you select **Revert Allocation** on a deployed license within the allocation grace period, which is 14 days after deployment, the license state changes to **Unlocked** so that you can reallocate the license to another system. • **Manage System** - Select a system, and then select this option to open the System Setup window, which you can use to configure firewall rules, interface roles, passwords, and system time. For more information, see "Access setting management" on page 36. • **Restart Web Server** - Select this option to restart the user interface, when required. For example, you might be required to restart your user interface after you install a new protocol that introduces new user interface components. • **Shutdown System** - Select a system, and then select this option to shut down the system. For more information, see "Shutting down a system" on page 36. • **Restart System** - Select a system, and then select this option to restart the system. For more information, see "Restarting a system" on page 35.

The Deployment Details pane provides information about your deployment. You can expand or collapse the Deployment Details pane.

Table 9. Deployment Details pane

Parameter	Details
Display	From this list box, select one of the following options: • **Licenses** - Displays a list of the allocated and deallocated licenses in your deployment. From this view, you can manage your licenses. • **Systems** - Displays a list of the host systems in your deployment. From this view, you can manage your systems.
Log Source Count	Displays the number of log sources that are configured for your deployment.
Users	Displays the number of users that are configured for your deployment.
Event Limit	Displays the total event rate limit your licenses allow for your deployment.
Flow Limit	Displays the total flow rate limit your licenses allow for your deployment.

When you select **Systems** from the **Display** list box in the Deployment Details pane, the System and License Management window displays the following information:

Table 10. System and License Management window parameters - Systems view.

Parameter	Description
Host Name	Displays the host name of this system.
Host IP	Displays the IP address of this system.
License Appliance Type	Displays the appliance type of this system.
Version	Displays the version number of the IBM Security QRadar software that this system uses.
Serial Number	Displays the serial number of this system, if available.
Host Status	Displays the status of this system, if available.
License Expiration Date	Displays the expiration date of the license that is allocated to this system.

Table 10. System and License Management window parameters - Systems view (continued).

Parameter	Description
License Status	Displays the status of the license that is allocated to this system. Statuses include: • **Unallocated** - Indicates that this license is not allocated to a system. • **Undeployed** - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet. • **Deployed** - Indicates that this license is allocated and active in your deployment. • **Unlocked** - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 10 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you must unlock a license after that period, contact Customer Support. • **Invalid** - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.
Event Rate Limit	Displays the event rate limit your license allows for this system.
Flow Rate Limit	Displays the flow rate limit your license allows for this system.

When you select **Licenses** from the **Display** list box in the Deployment Details pane, theSystem and License Management window displays the following information:

Table 11. System and License Management window parameters - Licenses view.

Parameter	Description
Host Name	Displays the host name of the system that is allocated to this license.
Host IP	Displays the IP address of the system that is allocated to this license.
Appliance Type	Displays the appliance type of the system that is allocated to this license.
License Identity	Displays the name of the IBM Security QRadar product this license provides.

Table 11. System and License Management window parameters - Licenses view (continued).

Parameter	Description
License Status	Displays the status of the license that is allocated to this system. Statuses include: • **Unallocated** - Indicates that this license is not allocated to a system. • **Undeployed** - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet. • **Deployed** - Indicates that this license is allocated and active in your deployment. • **Unlocked** - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 10 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you must unlock a license after that period, contact Customer Support. • **Invalid** - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.
License Expiration Date	Displays the expiration date of this license.
Event Rate Limit	Displays the event rate limit your license allows.
Flow Rate Limit	Displays the flow rate limit your license allows.

License management

You use the options available on the System and License Management window to manage your license keys.

About this task

A default license key provides you with access to the user interface for five weeks. You must allocate a license key to your system.

When you initially set up a system, you must complete the following tasks:

Procedure

1. Obtain a license key. Choose one of the following options for assistance with your license key:
   - For a new or updated license key, contact your local sales representative.
   - For all other technical issues, contact Customer Support.
2. Upload your license key. When you upload a license key, it is listed in the System and License Management window, but remains unallocated. For more information, see “Uploading a license key” on page 31
3. Allocate your license by choosing one of the following options:

- "Allocating a system to a license" on page 35
- "Allocating a license to a system"

4. Deploy your changes. From the **Admin** tab menu, click **Advanced** > **Deploy Full Configuration**.

Uploading a license key

You must upload a license key to the Console when you install a new QRadar system, update an expired license, or add a QRadar product, such as QRadar Vulnerability Manager, to your deployment.

Before you begin

Choose one of the following options for assistance with your license key:

1. For a new or updated license key, contact your local sales representative.
2. For all other technical issues, contact Customer Support.

About this task

If you log in to the user interface and your Console license key expired, you are automatically directed to the System and License Management window. You must upload a license key before you can continue. If one of your non-Console systems includes an expired license key, a message is displayed when you log in indicating a system requires a new license key. You must access the System and License Management window to update that license key.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. On the toolbar, click **Upload License**.
5. In the dialog box, click **Select File**.
6. On the File Upload window, locate and select the license key.
7. Click **Open**.
8. Click **Upload**.

Results

The license is uploaded to your Console and is displayed in the System and License Management window. By default, the license is not allocated.

What to do next

"Allocating a system to a license" on page 35

Allocating a license to a system

Use the options in the System and License Management window to allocate a license.

Before you begin

Before you begin, you must obtain and upload a license to your Console. See "Uploading a license key."

About this task

When you install a QRadar system, a default license key provides you with access to the user interface for five weeks. Before the default license expires, you must allocate a license key to your system. You can also add licenses to enable QRadar products, such as QRadar Vulnerability Manager.

License Status displays the status of the license that is allocated to this system. Statuses include:

- Unallocated - Indicates that this license is not allocated to a system.
- Undeployed - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet.
- Deployed - Indicates that this license is allocated and active in your deployment.
- Unlocked - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 14 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you must unlock a license after that period, contact Customer Support.
- Invalid - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Licenses**.
5. Select an unallocated license.
6. Click **Allocate System to License**.
7. Optional: To filter the list of licenses, type a keyword in the **Upload License** search box.
8. From the list of licenses, select a license.
9. Select a system.
10. Click **Allocate License to System**.

Reverting an allocation

You can revert an allocated license within the 14 day grace period.

About this task

After you allocate a license to a system and before you deploy your configuration changes, you can undo the license allocation. When you undo the license allocation, the license that was last allocated and deployed on the system is maintained.

Procedure

1. Click the**Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Licenses**.

5. Select the license that you want to revert.
6. Click **Actions** > **Revert Allocation**.

Viewing license details

A license key provides information and enforces the limits and abilities on an IBM Security QRadar system.

About this task

From the System and License Management window, you can view license details, such as the number of allowable log sources and the expiration dates.

Note: If you exceed the limit of configured logs sources, an error message is displayed. If log sources are auto-discovered and your limit is exceeded, they are automatically disabled. To extend the number of log sources, contact your sales representative.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Licenses**.
5. To display the **Current License Details** window for a license, double-click the license that you want to view.

What to do next

From the **Current License** window, you can complete the following tasks:

- Click **Upload Licences** to upload a license. See Uploading a license key.
- Click **Allocate License to System** on the toolbar to assign a license. See Allocating a system to a license.

Exporting a license

Export license key information to a desktop system.

About this task

You can export license key information to an external file on your desktop system.

Procedure

1. Click the **Admin tab**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Licenses**.
5. From the **Actions** menu, select **Export Licenses**.
6. Select one of the following options:
   - **Open with** - Opens the license key data using the selected application.
   - **Save File** - Saves the file to your desktop.
7. Click **OK**.

System management

Use the System and License Management window to manage systems in your deployment.

You use the options available on the System and License Management window to manage the systems in your deployment. You can view system details, assign a license to a system, or restart and shut down a system.

Viewing system details

View information about the system, including licenses from the System Details window.

About this task

Open the System Details window to view information about the system and the list of licenses that are allocated to the system.

The license list provides the following details for each license that is allocated to this system:

Table 12. License parameters

Header	Header
License Identity	Displays the name of the QRadar product this license provides.
License Status	Displays the status of the license that is allocated to this system. Statuses include: • Unallocated - Indicates that this license is not allocated to a system. • Undeployed - Indicates that this license is allocated to a system, but you have not deployed the allocation change. This means that the license is not active in your deployment yet. • Deployed - Indicates that this license is allocated and active in your deployment. • Unlocked - Indicates that this license has been unlocked. You can unlock a license if it has been deployed within the last 10 days. This is the default grace period to reallocate a license. After the grace period is passed, the license is locked to the system. If you need to unlock a license after that period, contact Customer Support. • Invalid - Indicates that this license is not valid and must be replaced. This status may indicate that your license has been altered without authorization.
License Appliance Types	Displays the appliance type that this license is valid for.
License Expiration Date	Displays the expiration date of this license.
Event Rate Limit	Displays the event rate limit this license allows.

Table 12. License parameters (continued)

Header	Header
Flow Rate Limit	Displays the flow rate limit this license allows.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. To display the system details, double-click the system that you want to view.

What to do next

From the system details window, you can complete the following tasks:

- Select a license and click **View License**. See "Viewing license details" on page 33.
- Click **Upload Licences** to upload a license. See "Uploading a license key" on page 31.
- Click **Allocate License to System** on the toolbar to assign a license. See "Allocating a system to a license."

Allocating a system to a license

After you obtain and upload a license, use the options in the System and License Management window to allocate a license.

You can allocate multiple licenses to a system. For example, in addition to the IBM Security QRadar SIEM, you can allocate IBM Security QRadar Risk Manager, and IBM Security QRadar Vulnerability Manager to your QRadar Console system.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select an available system.
6. Click **Allocate License to System**.
7. Optional: To filter the list of licenses, type a keyword in the Upload License search box.
8. From the list of licenses, select a license.
9. Select a system.
10. Click **Allocate License to System**.

Restarting a system

Use the **Restart System** option on the System and License Management window to restart a system in your deployment.

About this task

Data collection stops while the system is shutting down and restarting.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the system that you want to restart.
6. From the **Actions** menu, select **Restart System**.

Shutting down a system

Use the **Shutdown** option on the System and License Management window to shut down a system.

About this task

Data collection stops while the system is shutting down.

Procedure

1. Click the**Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the system that you want to shut down.
6. From the **Actions** menu, select **Shutdown**.

Exporting system details

About this task

Use the **Export Systems** option on the System and License Management window to export system information to an external file on your desktop system.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. From the **Actions** menu, select **Export Systems**.
6. Select one of the following options:
   - **Open with** - Opens the license key data by using the selected application.
   - **Save File** - Saves the file to your desktop.
7. Click **OK**.

Access setting management

You can use the System Setup window to configure firewall rules, interface roles, passwords, and system time.

If you require network configuration changes, such as an IP address change, to your Console and non-Console systems after your deployment is initially installed, you must use the **qchange_netsetup** utility to make these changes. For more information about network settings, see the *Installation Guide* for your product.

Configuring firewall access

You can configure local firewall access to enable communications between devices and IBM Security QRadar. Also, you can define access to the System Setup window.

About this task

Only the listed managed hosts that are listed in the **Device Access** box have access to the selected system. For example, if you enter one IP address, only that IP address is granted access to the Console. All other managed hosts are blocked.

If you change the **External Flow Source Monitoring Port** parameter in the QFlow configuration, you must also update your firewall access configuration. For more information about QFlow configuration, see Chapter 10, "Deployment editor," on page 115.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to configure firewall access settings.
6. From the **Actions** menu, select **Manage System**.
7. Log in to the System Setup window. The default is:
   a. **User Name:** `root`
   b. **Password:** `<password>` The user name and password are case sensitive.
8. From the menu, select **Managed Host Config** > **Local Firewall**.
9. Configure the following Device Access parameters:

Option	Description
Device Access	In the **Device Access** box, include any IBM systems that you want to access to this managed host. Only the listed managed hosts have access. For example, if you enter one IP address, only that IP address is granted access to the managed host. All other managed hosts are blocked.
IP Address	Type the IP address of the managed host you want to have access.
Protocol	Select the protocol that you want to enable access for the specified IP address and port. Options include: • **UDP** - Allows UDP traffic. • **TCP** - Allows TCP traffic. • **Any** - Allows any traffic.
Port	Type the port on which you want to enable communications.

10. Click **Allow**.
11. Configure the following System Administration Web Control parameter:

Table 13. System administration web control parameter

Parameter	Description
IP Address	Type the IP addresses of managed hosts that you want to allow access to the System Setup window in the **IP Address** field. Only listed IP addresses have access to the user interface. If you leave the field blank, all IP addresses have access. Make sure that you include the IP address of your client desktop you want to use to access the user interface. Failing to do so might affect connectivity.

12. Click **Allow** .
13. Click **Apply Access Controls** .
14. Wait for the System Setup window to refresh before you continue to another task.

Updating your host setup

You can use the System Setup window to configure the mail server you want to use and the global password for all systems in your QRadar deployment.

About this task

The global configuration password does not accept special characters. The global configuration password must be the same throughout your deployment. If you edit this password, you must also edit the global configuration password on all systems in your deployment.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to update your host setup settings.
6. From the **Actions** menu, select **Manage System.**
7. Log in to the System Setup window. The default is:
   a. User Name: `root`
   b. Password: `<password>`

      The user name and password are case-sensitive.
8. From the menu, select **Managed Host Config** > **QRadar Setup**.
9. In the **Mail Server** field, type the address for the mail server you want to use. QRadar SIEM uses this mail server to distribute alerts and event messages. To use the mail server that QRadar SIEM provides, type `localhost`.
10. In the **Enter the global configuration password**, type the password that you want to use to access the host. Type the password again for confirmation.

11. Click **Apply Configuration**.

Configuring interface roles

You can assign specific roles to the network interfaces on each managed host.

Before you begin

For assistance with determining the appropriate role for each interface, contact Customer Support.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to configure interface role settings.
6. From the **Actions** menu, select **Manage System.**
7. Log in to the System Setup window. The default is:
   a. User Name: `root`
   b. Password: `<password>`

   The user name and password are case-sensitive.
8. From the menu, select **Managed Host Config** > **Network Interfaces**.
9. For each listed network interface, select the role that you want to assign to the interface from the **Role** list box.
10. Click **Save Configuration**.
11. Wait for the System Setup window to refresh before you continue.

Changing passwords

You can change the root password for your system.

Before you begin

When you change a password, make sure that you record the entered values. The root password does not accept the following special characters: apostrophe ('), dollar sign ($), exclamation mark (!).

Procedure

1. Click the**Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to configure interface role settings.
6. From the **Actions** menu, select **Manage System**.
7. Log in to the System Setup window. The default is:
   a. User Name: `root`
   b. Password: `<password>`

   The user name and password are case-sensitive.
8. From the menu, select **Managed Host Config** > **Root Password**.

9. Update the password:
   a. **New Root Password** - Type the root password necessary to access the System Setup window.
   b. **Confirm New Root Password** - Type the password again for confirmation.
10. Click **Update Password**.

Time server configuration

You can configure your time server to use an RDATE server or you can manually configure your time server.

`System time overview`

All system time changes must be made within the System Time page. You can change the system time on the host that operates the Console. The change is then distributed to all managed hosts in your deployment.

You are able to change the time for the following options:

- System time
- Hardware time
- Time Zone
- Time Server

Configuring your time server using RDATE

Use the Time server sync tab to configure your time server using RDATE.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to configure system time settings.
6. From the **Actions** menu, select **Manage System**.
7. Log in to the System Setup window. The default is:
   a. User Name: `root`
   b. Password: `<password>`

   The user name and password are case-sensitive.
8. From the menu, select **Managed Host Config** > **System Time**.
9. Configure the time zone:
   a. Click the **Change time zone** tab.
   b. From the **Change timezone to** list box, select the time zone in which this managed host is located.
   c. Click **Save**.
10. Configure the time server:
    a. Click the **Time server sync** tab.

       Configure the following parameters:

Table 14. Time server parameters

Parameter	Description
Timeserver hostnames or addresses	Type the time server host name or IP address.
Set hardware time too	Select this check box if you want to set the hardware time.
Synchronize on schedule?	Select one of the following options: • No - Select this option if you do not want to synchronize the time. Go to step c. • Yes - Select this option if you want to synchronize the time.
Simple Schedule	Select this option if you want the time update to occur at a specific time. After you select this option, select a simple schedule from the list box.
Times and dates are selected below	Select this option to specify time you want the time update to occur. After you select this option, select the times and dates in the list boxes.

11. Click **Sync and Apply** .

Manually configuring time settings for your system

Use the options on the **Set time** and **Change timezone** tabs to manually configure your time settings.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** list box, select **Systems**.
5. Select the host for which you want to configure system time settings.
6. From the **Actions** menu, select **Manage System**.
7. Log in to the System Setupwindow. The default is:
   a. User Name: `root`
   b. Password: `<password>`

   The user name and password are case-sensitive.
8. From the menu, select **Managed Host Config** > **System Time**.
9. Click the **Set time** tab.

   The Set Time page is divided into tabs. You must save each setting before you continue. For example, when you configure system time, you must click **Apply** in the System Time pane before you continue.
10. Set the system time:
    a. Choose one of the following options:
       • In the System Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
       • Click **Set system time to hardware time**.
    b. Click **Apply**.
11. Set the hardware time:

a. Choose one of the following options:
   - In the Hardware Time pane, using the list boxes, select the current date and time you want to assign to the managed host.
   - Click **Set hardware time to system time**.

b. Click **Save**.

12. Configure the time zone:
    a. Click the **Change time zone** tab.
    b. From the **Change Timezone To** list box, select the time zone in which this managed host is located.
    c. Click **Save**.

Chapter 4. User information source configuration

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

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

User information source overview

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

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

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

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

User information sources

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

QRadar systems support the following user information sources:

Table 15. Supported information sources

Information Source	Information that is collected
Microsoft® Windows Active Directory (AD), version 2008 - Microsoft Windows AD is a directory service that authenticates and authorizes all users and computers that use your Windows network.	• full_name • user_name • user_principal_name • family_name • given_name • account_is_disabled • account_is_locked • password_is_expired • password_can_not_be_changed • no_password_expired • password_does_not_expire

Table 15. Supported information sources (continued)

Information Source	Information that is collected
IBM Security Access Manager (ISAM), version 7.0 - ISAM is an authentication and authorization solution for corporate web, client/server, and existing applications. For more information, see your IBM Security Access Manager (ISAM) documentation.	• name_in_rgy • first-name • last-name • account_valid • password_valid
IBM Security Identity Manager (ISIM), version 6.0 - ISIM provides the software and services to deploy policy-based provisioning solutions. This product automates the process of provisioning employees, contractors, and IBM Business Partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise. For more information, see your IBM Security Integration Manager (ISIM) documentation.	• Full name • DN

Reference data collections for user information

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

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

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

For example:

- `#`
- `# Domain Admins`
- `# key1,key2,data`
- ` smith_j,Full Name,John Smith`
- `smith_j,account_is_disabled,0`
- `smith_j,account_is_locked`
- `smith_j,password_does_not_expire,1`

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

Integration workflow example

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

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

Consider the following example:

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

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

1. Create a user information source for the ISIM server and collect ISIM Administrators user group information. This step creates a reference data collection that is called ISIM Administrators. See "Creating a user information source" on page 48.
2. Configure a building block to test for events in which the source IP address is the ISIM server and the user name is listed in the ISIM administrator reference data collection. For more information about building blocks, see the *User Guide* for your product.
3. Create an event search that uses the custom building block as a filter. For more information about event searches, see the *User Guide* for your product.
4. Create a custom report that uses the custom event search to generate daily reports on the audit activity of the privileged ISIM users. These generated reports indicate whether any ISIM administrator activity breaches your security policy. For more information about reports, see the *User Guide* for your product.

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

User information source configuration and management task overview

To initially integrate user information sources, you must perform the following tasks:

1. Configure a Tivoli Directory Integrator server. See "Configuring the Tivoli Directory Integrator server."
2. Create and manage user information sources. See "Creating and managing user information source" on page 48.
3. Collect user information. See "Collecting user information" on page 50.

Configuring the Tivoli Directory Integrator server

For QRadar SIEM to integrate with user information sources, you must install and configure a Tivoli Directory Integrator on a non-QRadar host.

About this task

No configuration is required on your system; however, you must access your Console to obtain the `QRadarIAM_TDI.zip` file. Then, install and configure a Tivoli Directory Integrator server on a separate host. If necessary, you must also create and import a self-signed certificate.

When you extract the QRadarIAM_TDI.zip file on the Tivoli Directory Integrator server, the TDI directory is automatically created. The TDI directory includes the following files:

- QradarIAM.sh, which is the TDI start up script for Linux
- QradarIAM.bat, which is the TDI start up script for Microsoft Windows
- QradarIAM.xml, which is the TDI xml script and must be stored in the same location as the QradarIAM.properties file
- QradarIAM.properties, which is the properties file for TDI xml script

When you install Tivoli Directory Integrator, you must configure a name for the Solutions directory. This task requires you to access the Solutions directory. Therefore, in the task steps, <solution_directory> refers to the name that you gave to the directory.

The following parameters are used to create and import certificates:

Table 16. Certification configuration parameters

Parameter	Description
<server_ip_address>	Defines the IP address of the Tivoli Directory Integrator server.
<days_valid>	Defines the number of days that the certificate is valid.
<keystore_file>	Defines the name of the keystore file.
-storepass <password>	Defines the password for keystore.
- keypass <password>	Defines the password for the private/public key pair.
<alias>	Defines the alias for an exported certificate.
<certificate_file>	Defines the file name of the certificate.

Procedure

1. Install Tivoli Directory Integrator on a non-QRadarhost. For more information on how to install and configure Tivoli Directory Integrator, see your Tivoli Directory Integrator (TDI) documentation.
2. Using SSH, log in to your Console as the root user.
   a. User name: root
   b. Password: <password>
3. Copy the QRadarIAM_TDI.zip file to the Tivoli Directory Integrator server.
4. On the Tivoli Directory Integrator server, extract the QRadarIAM_TDI.zip file in the Solutions directory.
5. Configure your Tivoli Directory Integrator server to integrate with QRadar.
   a. Open the Tivoli Directory Integrator <solution_directory>/solution.properties file.
   b. Uncomment the com.ibm.di.server.autoload property. If this property is already uncommented, note the value of the property.
   c. Choose one of the following options:
      - Change directories to the autoload.tdi directory, which contains the com.ibm.di.server.autoload property by default.
      - Create an autoload.tdi directory in the <solution_directory> to store the com.ibm.di.server.autoload property.

d. Move the TDI/QRadarIAM.xml and TDI/QRadarIAM.property files from the Tivoli Directory Integrator directory to <solution_directory>/autoload.tdi directory or the directory you created in the previous step.

e. Move the `QradarIAM.bat` and `QradarIAM.sh` scripts from the Tivoli Directory Integrator directory to the location from which you want to start the Tivoli Directory Integrator.

6. If certificate-based authentication is required for your system to authenticate to the Tivoli Directory Integrator, select one of the following options:
   - To create and import a self-signed certificate, see Step 7.
   - To import a CA certificate, see Step 8.
7. Create and import the self-signed certificate into the Tivoli Directory Integrator truststore.
   a. To generate a keystore and a private/public key pair, type the following command:
      - `keytool -genkey -dname cn=<server_ip_address> -validity <days_valid> -keystore <keystore_file> -storepass <password> -keypass <password>`
      - For example, `keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret`

   b. To export the certificate from the keystore, type the following command:
      - `keytool -export -alias <alias> -file <certificate_file> -keystore <keystore_file> - storepass <password>`
      - For example, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`

   c. To import the primary certificate back into the keystore as the self-signed CA certificate, type the following command:
      - `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
      - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`

   d. Copy the certificate file to the `/opt/qradar/conf/trusted_certificates` on the QRadar SIEM Console.
8. Import the CA certificate into the Tivoli Directory Integrator truststore.
   a. To import the CA certificate into the keystore as the self-signed CA certificate, type the following command:
      - `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
      - For example, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`

   b. Copy the CA certificate file to the `/opt/qradar/conf/trusted_certificates` on the QRadar SIEM Console.
9. Edit the <solution_directory>/solution.properties file to uncomment and configure the following properties:
   - javax.net.ssl.trustStore=<keystore_file>
   - {protect}-javax.net.ssl.trustStorePassword=<password>
   - javax.net.ssl.keyStore=<keystore_file>
   - {protect}-javax.net.ssl.keyStorePassword=<password>

Note: The default current, unmodified password might be displayed in the following format: {encr}EyHbak. Enter the password as plain text. The password is encryps the first time that you start Tivoli Directory Integrator.

10. Use one of the following scripts to start the Tivoli Directory Integrator:
    - QradarIAM.sh for Linux
    - QradarIAM.bat for Microsoft windows

Creating and managing user information source

Use the UISConfigUtli utility to create, retrieve, update, or delete user information sources.

Use the UISConfigUtli utility to create, retrieve, update, or delete user information sources.

Creating a user information source

Use the UISConfigUtli utility to create a user information source.

Before you begin

Before you create a user information source, you must install and configure your Tivoli Directory Integrator server. For more information, see "Configuring the Tivoli Directory Integrator server" on page 45.

About this task

When you create a user information source, you must identify the property values required to configure the user information source. The following table describes the supported property values:

Table 17. Supported user interface property values

Header	Header
tdiserver	Defines the host name of the Tivoli Directory Integrator server.
tdiport	Defines the listening port for the HTTP connector on the Tivoli Directory Integrator server.
hostname	Defines the host name of the user information source host.
port	Defines the listening port for the Identity and Access Management registry on the user information host.
username	Defines the user name that QRadar SIEM uses to authenticate to the Identity and Access Management registry.
password	Defines the password that is required to authenticate to the Identity and Access Management registry.
searchbase	Defines the base DN.
search filter	Defines the search filter that is required to filter the user information that is retrieved from the Identity and Access Management registry.

Procedure

1. Using SSH, log in to your Console as the root user.
   a. User name: `root`
   b. Password: `<password>`
2. To add a user information source, type the following command:
   `UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2...,propn=valuen]`

   Where:

   - `<name>` Is the name of the user information source you want to add.
   - `<AD|ISAM|ISIM|ISFIM>` Indicates the user information source type.
   - `[-d description]` Is a description of the user information source. This parameter is optional.
   - `[-p prop1=value1,prop2=value2,...,propn=valuen]` Identifies the property values required for the user information source. For more information about the supported parameters, see "Creating a user information source" on page 48.

   For example:

   - `/UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p "tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,hostname=vmibm7094.ottaw`

Retrieving user information sources

Use the UISConfigUtli utility to retrieve user information sources.

Procedure

1. Using SSH, log in to your Console as the root user.
   a. User name: `root`
   b. Password: `<password>`
2. Choose one of the following options:
   a. Type the following command to retrieve all user information sources:
      `UISConfigUtil.sh get <name>`
   b. Type the following command to retrieve a specific user information source:
      `UISConfigUtil.sh get <name>`

      Where `<name>` is the name of the user information source you want to retrieve.

      For example:

      `[root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"`

Editing a user information source

Use the UISConfigUtli utility to edit a user information source.

Procedure

1. Using SSH, log in to your Console as the root user.
   a. User name: `root`
   b. Password: `<password>`
2. Type the following command to edit a user information source:
   `UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2,...,propn=valuen]`

Where:

- <name> Is the name of the user information source you want to edit.
- <AD|ISAM|ISIM|ISFIM> Indicates the user information source type. To update this parameter, type a new value.
- [-d description] Is a description of the user information source. This parameter is optional. To update this parameter, type a new description.
- [-p prop1=value1,prop2=value2,...,propn=valuen] Identifies the property values required for the user information source. To update this parameter, type new properties. For more information about the supported parameters, see "Creating a user information source" on page 48.

For example:

```
./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p
"searchbase=DC=local"
```

Deleting a user information source

Use the UISConfigUtli utility to edit a user information source.

Procedure

1. Using SSH, log in to your Console as the root user.
   a. User name: root
   b. Password: <password>
2. Type the following command to delete a user information source:
   UISConfigUtil.sh delete <name>
   Where <name> is the name of the user information source you want to delete.

What to do next

The collected user information is stored in a reference data collection on the IBM Security QRadar SIEMdatabase. If no reference date collection exists, a new reference data collection is created. If a reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see Reference data collections for user information.

Collecting user information

Use the GetUserInfo utility to collect user information from the user information sources and store the data in a reference data collection.

About this task

Use this task to collect user information on demand. If you want to create automatic user information collection on a schedule, create a cron job entry. For more information about cron jobs, see your Linux documentation.

Procedure

1. Using SSH, log in to your Console as the root user.
   a. User name: root
   b. <password>
2. Type the following command to collect user information on demand:
   GetUserInfo.sh <UISName>

Where <UISName> is the name of the user information source you want to collect information from.

What to do next

The collected user information is stored in a reference data collection on the database. If no reference date collection exists, a new reference data collection is created. If a reference data collection was previously created for this user information source, the reference map is purged of previous data and the new user information is stored. For more information about reference data collections, see "Reference data collections for user information" on page 44.

Chapter 5. Set up QRadar SIEM

Use the features on the **Admin** tab to set up IBM Security QRadar SIEM.

You can configure your network hierarchy, automatic updates, system settings, event and flow retention buckets, system notifications, console settings, offense close reasons, and index management.

Network hierarchy

QRadar uses the network hierarchy to understand your network traffic and provide you with the ability to view activity for your entire deployment.

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

When you define your network hierarchy, you must consider the systems, users, and servers that can be grouped.

You can group systems and user groups that have similar behavior. However, do not group a server that has unique behavior with other servers on your network. Placing a unique server alone provides the server greater visibility in QRadar, and you can manage specific policies.

Within a group, you can place servers with high volumes of traffic, such as mail servers, at the top of the group. This hierarchy provides you with a visual representation when a discrepancy occurs.

If your deployment processes more than 600,000 flows, then you can create multiple top-level groups.

You can organize your systems and networks by role or similar traffic patterns. For example, mail servers, departmental users, labs, or development groups. Using this organization, you can differentiate network behavior and enforce network management security policies.

Large network groups can cause you difficulty when you view detailed information for each object. Do not configure a network group with more than 15 objects.

Combine multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network group to conserve disk space. For example:

Table 18. Example of multiple CIDRs and subnets in a single network group

Group	Description	IP addresses
1	Marketing	10.10.5.0/24
2	Sales	10.10.8.0/21

Table 18. Example of multiple CIDRs and subnets in a single network group (continued)

Group	Description	IP addresses
3	Database Cluster	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

Add key servers as individual objects and group other major but related servers into multi-CIDR objects.

Define an all-encompassing group so when you define new networks, the appropriate policies, and behavioral monitors are applied. For example:

Table 19. Example of an all-encompassing group

Group	Subgroup	IP address
Cleveland	Cleveland miscellaneous	10.10.0.0/16
Cleveland	Cleveland Sales	10.10.8.0/21
Cleveland	Cleveland Marketing	10.10.1.0/24

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

Acceptable CIDR values

QRadar accepts specific CIDR values.

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

Table 20. Acceptable CIDR values

CIDR Length	Mask	Number of Networks	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068

Table 20. Acceptable CIDR values (continued)

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

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

- 209.60.128.0 is a class C network address with a mask of /24.
- 209.60.128.0 /22 is a supernet that yields:
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25

  Subnet Host Range

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254
- 192.0.0.0 /26

  Subnet Host Range

  0 192.0.0.1 - 192.0.0.62

  1 192.0.0.65 - 192.0.0.126

  2 192.0.0.129 - 192.0.0.190

  3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27

  Subnet Host Range

  0 192.0.0.1 - 192.0.0.30

1 192.0.0.33 - 192.0.0.62

2 192.0.0.65 - 192.0.0.94

3 192.0.0.97 - 192.0.0.126

4 192.0.0.129 - 192.0.0.158

5 192.0.0.161 - 192.0.0.190

6 192.0.0.193 - 192.0.0.222

7 192.0.0.225 - 192.0.0.254

Related tasks:

"Defining your network hierarchy"
Use the Network Views window to define your network hierarchy.

Defining your network hierarchy

Use the Network Views window to define your network hierarchy.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Network Hierarchy**.
4. From the menu tree on the Network Views window, select the area of the network in which you want to add a network object.
5. Click **Add**.
6. From **Group** list, select the group in which you want to add the new network object.
7. Optional: Click **Add Group** to create a new group.
8. Type a unique name for the object.
9. Type or select the weight of the object. The range is 0 - 100 and indicates the importance of the object in the system.
10. Type the CIDR range for this object and click **Add**.
11. Type a description for this network object.
12. Click **Select Color** and select a color for this object.
13. Select the database length.
14. Click **Save**.
15. Repeat for all network objects.
16. Optional: Click **Re-Order** and organize the network objects.

Related concepts:

"Acceptable CIDR values" on page 54
QRadar accepts specific CIDR values.

Automatic updates

You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

QRadar uses system configuration files to provide useful characterizations of network data flows.

The Console must be connected to the Internet to receive the updates. If your Console is not connected to the Internet, you must configure an internal update server for your Console to download the files from.

Update files are available for manual download from the following website:

http://www.ibm.com/support/fixcentral/

Update files can include the following updates:

- Configuration updates, which include configuration file changes, vulnerability, QID map, and security threat information updates.
- DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, which include items such as updated JAR files.
- Minor updates, which include items such as more Online Help content or updated scripts.

To maintain the integrity of your current configuration and information, either replace your existing configuration files or integrate the updated files with your existing files.

After you install updates on your Console and deploy your changes, the Console updates its managed hosts if your deployment is defined in your deployment editor. For more information about the deployment editor, see Chapter 10, "Deployment editor," on page 115.

CAUTION:
You must build your system and event views in the deployment editor before you configure automatic or manual updates. Otherwise, your managed hosts are not updated.

Related concepts:

"Set up a QRadar update server" on page 62
If your deployment includes a QRadar Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a QRadar update server to manage the update process.

Viewing pending updates

Your system is preconfigured for weekly automatic updates. You can view the pending updates in the Updates window.

About this task

Your system needs to be operational long enough to retrieve the weekly updates. If no updates are displayed in the Updates window, either your system has not been in operation long enough to retrieve the weekly updates or no updates have been issued. If this occurs, you can manually check for new updates. For more information about checking for new updates, see "Checking for new updates" on page 60.

The **Check for Updates** toolbar provides the following functions:

Table 21. Check for Updates toolbar functions

Function	Description
Hide	Select one or more updates, and then click **Hide** to remove the selected updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page. For more information, see “Restoring hidden updates” on page 61.
Install	You can manually install updates. When you manually install updates, the installation process starts within a minute. For more information, see“Manually installing automatic updates” on page 61.
Schedule	You can configure a specific date and time to manually install selected updates on your Console. Scheduling is useful when you want to schedule the update installation during off-peak hours. For more information, see “Scheduling an update” on page 60.
Unschedule	You can remove preconfigured schedules for manually installing updates on your Console. For more information, see“Scheduling an update” on page 60.
Search By Name	You can locate a specific update by name.
Next Refresh	This counter displays the amount of time until the next automatic refresh. The list of updates on the Check for Updates page automatically refreshes every 60 seconds. The timer is automatically paused when you select one or more updates.
Pause	Pauses the automatic refresh process. To resume automatic refresh, click **Play**.
Refresh	Refreshes the list of updates.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. To view details on an update, select the update.

Configuring automatic update settings

You can customize the automatic update settings to change the frequency, update type, server configuration, and backup settings.

About this task

You can select the **Auto Deploy** to automatically deploy updates. If **Auto Deploy** is not selected, then you must manually deploy changes, from the **Dashboard** tab, after updates are installed.

You can select **Auto Restart Service** to allow automatic updates that require the user interface to restart. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the updated from the Check for Updates window.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **Change Settings**.
5. On the **Basic** tab, select the schedule for updates.
6. In the **Configuration Updates** section, select the method that you want to use for updating your configuration files.
7. In the **DSM, Scanner, Protocol Updates** section, select an option to install updates.
8. In the **Major Updates** section, select an option for receiving major updates for new releases.
9. In the **Minor updates** section, select an option for receiving patches for minor system issues.
10. Select the **Auto Deploy** check box if you want to deploy update changes automatically after updates are installed.
11. Select the **Auto Restart Service** check box if you want to restart the user interface service automatically after updates are installed.
12. Click the **Advanced** tab.
13. In **Web Server**field, type the web server from which you want to obtain the updates. The default web server is http://www.ibm.com/support/fixcentral.
14. In the **Directory field**, type the directory location on which the web server stores the updates. The default directory is `autoupdates/`.
15. Optional: In the **Proxy Server** field, type the URL for the proxy server. The proxy server is required if the application server uses a proxy server to connect to the Internet.
16. Optional: In the **Proxy Username** field, type the user name for the proxy server. A user name is required if you are using an authenticated proxy.
17. In the **Proxy Password** field, type the password for the proxy server. A password is required if you are using an authenticated proxy.
18. Select the **Send Feedback** check box if you want to send feedback to IBM about the update. If errors occur during an update, feedback is automatically sent by a web form.
19. In the **Backup Retention Period** list, type or select the number of days that you want to store files that are replaced during the update process. The files are stored in the location that is specified in the **Backup Location**. The minimum is one day and the maximum is 65535 years.
20. In the **Backup Location** field, type the location where you want to store backup files.
21. In the **Download Path** field, type the directory path location to which you want to store DSM, minor, and major updates. The default directory path is `/store/configservices/staging/updates`.
22. Click **Save**.

Scheduling an update

Automatic updates occur on a recurring schedule according to the settings on the Update Configuration page. You can also schedule an update or a set of updates to run at a specific time.

About this task

To reduce performance impacts on your system, schedule a large update to run during off-peak hours.

For detailed information on each update, you can select the update. A description and any error messages are displayed in the right pane of the window.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click**Auto Update**.
4. Optional: If you want to schedule specific updates, select the updates that you want to schedule.
5. From the **Schedule** list box, select the type of update you want to schedule.
6. Using the calendar, select the start date and time of when you want to start your scheduled updates.

Clearing scheduled updates

You can cancel any scheduled update.

About this task

Scheduled updates display a status of **Scheduled** in the **Status** field. After the schedule is cleared, the status of the update displays as **New**.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **Check for Updates**.
5. Optional: If you want to clear specific scheduled updates, select the updates that you want to clear.
6. From the **Unschedule** list box, select the type of scheduled update that you want to clear.

Checking for new updates

IBM provides updates on a regular basis. By default, the Auto Update feature is scheduled to automatically download and install updates. If you require an update at a time other than the preconfigured schedule, you can download new updates.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.

4. On the navigation menu, click **Check for Updates**.
5. Click **Get new updates**.

Manually installing automatic updates

IBM provides updates regularly. By default, updates are automatically downloaded and installed on your system. However, you can install an update at a time other than the preconfigured schedule.

About this task

The system retrieves the new updates from Fix Central. This might take an extended period. When complete, new updates are listed on the Updates window.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **Check for Updates**.
5. Optional: If you want to install specific updates, select the updates that you want to schedule.
6. From the **Install** list box, select the type of update you want to install.

Viewing your update history

After an update was successfully installed or failed to install, the update is displayed on the View Update History page.

About this task

A description of the update and any installation error messages are displayed in the right pane of the View Update History page. The View Update History page provides the following information:

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **View Update History**.
5. Optional: Using the **Search by Name** text box, you can type a keyword and then press Enter to locate a specific update by name.
6. To investigate a specific update, select the update.

Restoring hidden updates

You can remove updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **Restore Hidden Updates**.

5. Optional: To locate an update by name, type a keyword in the **Search by Name** text box and press Enter.
6. Select the hidden update that you want to restore.
7. Click **Restore**.

Viewing the autoupdate log

The autoupdate log contains the most recent automatic update that was run on your system.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Auto Update**.
4. On the navigation menu, click **View Log**.

Set up a QRadar update server

If your deployment includes a QRadar Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a QRadar update server to manage the update process.

The autoupdate package includes all files necessary to manually set up an update server in addition to the necessary system configuration files for each update. After the initial setup, you only need to download and uncompress the most current autoupdate package to manually update your configuration.

You can subscribe to notifications in Fix Central to receive notification of new updates.

Related concepts:

"Automatic updates" on page 56
You can automatically or manually update your configuration files to ensure that your configuration files contain the latest network security information.

Configuring your update server

Use this task to configure an Apache server. You must create an update directory and download the autoupdate package from Fix Central.

About this task

Autoupdates are available in Fix Central.

Procedure

1. Access your Apache server. By default, the update directory is in the web root directory of the Apache server. You can place the directory in another location if you configure QRadar accordingly.
2. Create an update directory named `autoupdates/`.
3. Optional: Create an Apache user account and password to be used by the update process.
4. Download the autoupdate package from Fix Central: http://www.ibm.com/support/fixcentral You can find QRadar products in the Security Systems **Product Group** list on Fix Central.

5. Save the autoupdate package file on your Apache server in the `autoupdates/` directory that you created.
6. On the Apache server, type the following command to uncompress the autoupdate package.**`tar -zxf updatepackage-[timestamp].tgz`**
7. Click the **Admin** tab.
8. On the navigation menu, click **System Configuration**.
9. Click **Auto Update**.
10. Click **Change Settings**.
11. Select the **Advanced tab**.
12. To direct the update process to the Apache server, configure the following parameters in the **Server Configuration** panel:
    a. In **Web Server**field, type the address or directory path of your Apache server. If the Apache server runs on non-standard ports, add `:<portnumber>` to the end of the address. `https://qmmunity.q1labs.com/:8080`
    b. In the **Directory field**, type the directory location on which the web server stores the updates. The default directory is `autoupdates/`.
    c. Optional: In the **Proxy Server** field, type the URL for the proxy server. The proxy server is required if the application server uses a proxy server to connect to the Internet.
    d. Optional: In the **Proxy Username** field, type the user name for the proxy server. A user name is required if you are using an authenticated proxy.
    e. Optional: In the **Proxy Password** field, type the password for the proxy server. A password is required if you are using an authenticated proxy.
13. Select **Deploy changes**.
14. Click **Save**.
15. Using SSH, log in to QRadar as the root user.
16. Type the following command to configure the user name that you set for your Apache server: **`/opt/qradar/bin/UpdateConfs.pl -change_username <username>`**
17. Type the following command to configure the password that you set for your Apache server: **`/opt/qradar/bin/UpdateConfs.pl -change_password <password>`**
18. Test your update server by typing the command:**`lynx https://<your update server>/<directory path to updates>/manifest_list`**
19. Type the user name and password.

Configuring your QRadarConsole as the Update Server

You can configure your QRadar Console to be your update server.

About this task

To configure your QRadar console to be your upgrade server, you complete three tasks:

- Create an autoupdate directory.
- Download the autoupdate package from Fix Central.
- Configure QRadar to accept the autoupdates.

Procedure

1. Log in to QRadar as the root user.

2. Type the following command to create the autoupdate directory: **mkdir /opt/qradar/www/autoupdates/**
3. Download the autoupdate package from Fix Central: http://www.ibm.com/support/fixcentral You can find QRadar products in the Security Systems **Product Group** list on Fix Central.
4. Save the autoupdate package file on your Apache server in the `autoupdates/` directory that you created.
5. On your QRadar Console, type the following command to uncompress the autoupdate package.**tar -zxf updatepackage-[timestamp].tgz**
6. Log in to QRadar user interface.
7. On the navigation menu, click **System Configuration**.
8. Click **Auto Update**.
9. Click **Change Settings**.
10. Select the **Advanced tab**.
11. In **Web Server**field, type `https://localhost/`.
12. Clear the **Send feed** check box.

Adding new updates

You can download updates from Fix Central to your update server.

Before you begin

You must configure your update server and set up QRadar to receive updates from the update server.

Procedure

1. Download the autoupdate package from Fix Central: http://www.ibm.com/support/fixcentral You can find QRadar products in the Security Systems **Product Group** list on Fix Central.
2. Save the autoupdate package file on your update server in the `autoupdates/` directory that you created.
3. Type the following command to uncompress the autoupdate package.**tar -zxf updatepackage-[timestamp].tgz**
4. Log in to QRadar as the root user.
5. Type the following command to test your update server, **lynx https://<your update server>/<directory path to updates>/manifest_list**.
6. Type the user name and password of your update server.

Configuring system settings

You can configure system settings.

About this task

On the System Settings window, you can configure the following parameters:

Table 22. System Settings window parameters

Parameter	Description
System Settings	

Table 22. System Settings window parameters (continued)

Parameter	Description
Administrative Email Address	The email address of the designated system administrator. The default email address is root@localhost.
Alert Email From Address	The email address from which you want to receive email alerts. This address is displayed in the **From** field of the email alerts. A valid address is required by most email servers. The default email address is root@<hostname.domain>.
Resolution Interval Length	The resolution interval length determines at what interval the QRadar QFlow Collector and Event Collectors send bundles of information to the Console. If you select the 30-seconds option, results display on the QRadar user interface as the data enters the system. However, with shorter intervals, the volume of time series data is larger and the system might experience delays in processing the information.
Delete Root Mail	Root mail is the default location for host context messages.
Temporary Files Retention Period	The period that you want the system to retain temporary files. The default storage location for temporary files is the `/store/tmp` directory.
Asset Profile Query Period	The period for an asset search to process before a timeout occurs.
Coalescing Events	The coalesce log settings for events. Select **Yes** to enable log sources to coalesce, or bundle, events. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the **Coalescing Event** parameter in the log source configuration. For more information, see the Managing Log Sources Guide.
Store Event Payload	Log sources can store event payload information. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the **Event Payload** parameter in the log source configuration. For more information, see the *Managing Log Sources Guide* users guide.
Global Iptables Access	The IP addresses of non-Console systems that do not have iptables configuration to which you want to enable direct access. To enter multiple systems, type a comma-separated list of IP addresses.

Table 22. System Settings window parameters (continued)

Parameter	Description
Syslog Event Timeout (minutes)	The amount of time that the status of a syslog device is recorded as an error if no events are received within the timeout period. The status is displayed on the Log Sources window.
Partition Tester Timeout (seconds)	The amount of time for a partition test to perform before a timeout occurs.
Max Number of TCP Syslog Connections	The maximum number of Transmission Control Protocol (TCP) syslog connections you want to allow your system.
Export Directory	The location where offense, event, and flow exports are stored. The default location is `/store/exports`.
Display Country/Region Flags	If geographic information is available for an IP address, the country or region is visually indicated by a flag. You can select **No** from this list box disable this feature.
Database Settings	
User Data Files	The location of the user profiles. The default location is `/store/users`.
Accumulator Retention - Minute-By-Minute	The period that you want to retain minute-by-minute data accumulations. Every 60 seconds, the data is aggregated into a single data set.
Accumulator Retention - Hourly	The period that you want to retain hourly data accumulations. At the end of every hour, the minute-by minute data sets are aggregated into a single hourly data set.
Accumulator Retention - Daily	The period that you want to retain daily data accumulations. At the end of every day, the hourly data sets are aggregated into a single daily data set.
Payload Index Retention	The amount of time you want to store payload indexes. For more information about payload indexing, see the *Enabling Payload Indexing for Quick Filtering Technical Note*.

Table 22. System Settings window parameters (continued)

Parameter	Description
Offense Retention Period	The period that you want to retain closed offense information. The default setting is 3 days. The minimum is 1 day and the maximum is 2 years. After the offense retention period elapses, closed offenses are purged from the database. Offenses can be retained indefinitely if they are not closed or inactive, and they are still receiving events. The magistrate automatically marks an offense as Inactive if the offense has not received an event for 5 days. This 5-day period is known as the dormant time. If an event is received during the dormant time, the dormant time is reset back to zero. When an offense is closed either by you (Closed) or the magistrate (Inactive), the **Offense Retention Period** setting is applied.
Attacker History Retention Period	From the list box, select the amount of time that you want to store the attacker history.
Target Retention Period	From the list box, select the amount of time that you want to store the target history.
Ariel Database Settings	
Flow Data Storage Location	The location that you want to store the flow log information. The default location is `/store/ariel/flows`.
Log Source Storage Location	The location where you want to store the log source information. The default location is `/store/ariel/events`.
Search Results Retention Period	The amount of time you want to store search results.
Reporting Max Matched Results	The maximum number of results you want a report to return.
Command Line Max Matched Results	The maximum number of results you want the AQL command line to return.
Web Execution Time Limit	The maximum amount of time, in seconds, you want a query to process before a timeout occurs.
Reporting Execution Time Limit for Manual Reports	The maximum amount of time, in seconds, you want a reporting query to process before a timeout occurs.
Command Line Execution Time Limit	The maximum amount of time, in seconds, you want a query in the AQL command line to process before a timeout occurs.
Web Last Minute (Auto refresh) Execution Time Limit	The maximum amount of time, in seconds, you want an auto refresh to process before a timeout occurs.

Table 22. System Settings window parameters (continued)

Parameter	Description
Flow Log Hashing	Stores a hash file for every stored flow log file. Select **Yes** to enable logging.
Event Log Hashing	Stores a hash file for every stored event log file. Select **Yes** to enable logging.
HMAC Encryption	This parameter only displays when the **Event Log Hashing** or **Flow Log Hashing** system setting is enabled. Select **Yes** to allow QRadar to encrypt the integrity hashes on stored event and flow log files.
HMAC Key	The key that you want to use for HMAC encryption. The key must be unique. This parameter only displays when the **HMAC Encryption** system setting is enabled.
Verify	This parameter only displays when the **HMAC Encryption** system setting is enabled. Retype the key that you want to use for HMAC encryption. The key must match the key that you typed in the **HMAC Key** field.

Table 22. System Settings window parameters (continued)

Parameter	Description
Hashing Algorithm	You can use a hashing algorithm for database integrity. QRadar uses the following hashing algorithm types: • **Message-Digest Hash Algorithm** - Transforms digital signatures into shorter values called Message-Digests (MD). • **Secure Hash Algorithm (SHA) Hash Algorithm** - Standard algorithm that creates a larger (60 bit) MD. • From the list box, select the log hashing algorithm that you want to use for your deployment. If the **HMAC Encryption** parameter is disabled, the following options are available: • **MD2** - Algorithm that is defined by RFC 1319. • **MD5** - Algorithm that is defined by RFC 1321. • **SHA-1** - Algorithm that is defined by Secure Hash Standard (SHS), NIST FIPS 180-1. This is the default setting. • **SHA-256** - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-256 is a 255-bit hash algorithm that is intended for 128 bits of security against security attacks. • **SHA-384** - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-384 is a bit hash algorithm, created by truncating the SHA-512 output. • **SHA-512** - Algorithm that is defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-512 is a bit hash algorithm that is intended to provide 256 bits of security. If the **HMAC Encryption** parameter is enabled, the following options are available: • **HMAC-MD5 -** An encryption method that is based on the MD5 hashing algorithm. • **HMAC-SHA-1** - An encryption method that is based on the SHA-1 hashing algorithm. • **HMAC-SHA-256 -** An encryption method that is based on the SHA-256 hashing algorithm. • **HMAC-SHA-384 -** An encryption method that is based on the SHA-384 hashing algorithm. • **HMAC-SHA-512** An encryption method that is based on the SHA-512 hashing algorithm.

Table 22. System Settings window parameters (continued)

Parameter	Description
Transaction Sentry Settings	
Transaction Max Time Limit	A transaction sentry detects unresponsive applications using transaction analysis. If an unresponsive application is detected, the transaction sentry attempts to return the application to a functional state. The length of time you want the system to check for transactional issues in the database.
Resolve Transaction on Non-Encrypted Host	The transaction sentry can resolve all error conditions that are detected on the Console or non-encrypted managed hosts. If you select **No**, the conditions are detected and logged but you must manually intervene and correct the error.
Resolve Transaction on Encrypted Host	The transaction sentry can resolve all error conditions that are detected on the encrypted managed host. If you select **No**, the conditions are detected and logged but you must manually intervene and correct the error.
SNMP Settings	
SNMP Version	The version of SNMP that you want to use. Disable this setting if you do not want SNMP responses in the QRadar custom rules engine.
SNMPv2c Settings	
Destination Host	The IP address to which you want to send SNMP notifications.
Destination Port	The port number to which you want to send SNMP notifications.
Community	The SNMP community, such as public.
SNMPv3 Settings	
Destination Host	The IP address to which you want to send SNMP notifications.
Destination Port	The port to which you want to send SNMP notifications.
Username	The name of the user you want to access SNMP-related properties.
Security Level	The security level for SNMP.
Authentication Protocol	The algorithm that you want to use to authenticate SNMP traps.
Authentication Password	The password that you want to use to authenticate SNMP traps.
Privacy Protocol	The protocol that you want to use to decrypt SNMP traps.

Table 22. System Settings window parameters (continued)

Parameter	Description
Privacy Password	The password that is used to decrypt SNMP traps.
Embedded SNMP Daemon Settings	
Enabled	Enables access to data from the SNMP Agent using SNMP requests. After you enable the embedded SNMP daemon, you must access the host that is specified in the **Destination Host** parameter and type `qradar` in the **Username** field. A password is not required. The location where you configure a destination host to communicate with QRadar SIEM can vary depending on the vendor host. For more information on configuring your destination host to communicate with QRadar, see your vendor documentation.
Daemon Port	The port that you want to use for sending SNMP requests.
Community String	The SNMP community, such as **public.** This parameter applies only if you are using SNMPv2 and SNMPv3.
IP Access List	The systems that can access data from the SNMP agent using an SNMP request. If the **Enabled** option is set to Yes, this option is enforced.
IF-MAP Client/Server Settings	
IF-MAP Version	The version of IF-MAP that you require. The Interface For Metadata Access Points (IF-MAP) rule response enables IBM Security QRadar SIEMto publish alert and offense data derived from events, flows, and offense data on an IF-MAP server. If this setting is disabled, the other IF-MAP Client/Server settings are not displayed.
Server Address	The IP address of the IF-MAP server.
Basic Server Port	The port number for the basic IF-MAP server.
Credential Server Port	The port number for the credential server. .
Authentication	The type of authentication that you require. Before you can configure IF-MAP authentication, you must configure your IF-MAP server certificate. For more information on how to configure your IF-MAP certificate, see “Configuring your IF-MAP server certificates” on page 73.

Table 22. System Settings window parameters (continued)

Parameter	Description
Key Password	The key password to be shared between the IF-MAP client and server. This setting is displayed only when you select the **Mutual** option for the **Authentication** setting.
Username	The user name that is required to access the IF-MAP server. This setting is displayed only when you select the **Basic** option for the **Authentication** setting.
User Password	The password that is required to access the IF-MAP server. This setting is displayed only when you select the **Basic** option for the **Authentication** setting.
Asset Profile Settings This pane is only displayed if IBM Security QRadar Vulnerability Manager is installed on your system.	
Asset Profile Retention Period	The period, in days, that you want to store the asset profile information. The **Use Advanced** setting enables QRadar to apply advanced, granular database retention logic to asset data. If you want to apply one retention period to all asset data, you can configure this system setting.
Enable DNS Lookups for Host Identity	Enables QRadar to run Domain Name System (DNS) lookups for host identity.
Enable WINS Lookups for Host Identity	Enables QRadar to run Windows Internet Name Service (WINS) lookups for host identity.
Asset Profile Reporting Interval	The interval, in seconds, that the database stores new asset profile information.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System Settings** icon.
4. Configure the system settings.
5. Click **Save**.
6. On the **Admin** tab menu, select **Advanced** > **Deploy Full Configuration**.

Configuring your IF-MAP server certificates

Before you can configure IF-MAP authentication on the System Settings window, you must configure your IF-MAP server certificate.

Configuring IF-MAP Server Certificate for Basic Authentication

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

Before you begin

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

Procedure

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

Configuring IF-MAP Server Certificate for Mutual Authentication

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

Before you begin

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

Mutual authentication requires certificate configuration on your Console and your IF-MAP server. For assistance configuring the certificate on your IF-MAP server, contact your IF-MAP server administrator.

Procedure

1. Using SSH, log in to QRadar as the root user.
2. Access the certificate to the `/opt/qradar/conf/trusted_certificates` directory
3. Copy the SSL intermediate certificate and SSL Verisign root certificate to your IF-MAP server as CA certificates. For assistance, contact your IF-MAP server administrator.
4. Type the following command to create the Public-Key Cryptography Standards file with the .pkcs12 file extension using the following command:`openssl pkcs12 -export -inkey <private_key> -in <certificate> -out <pkcs12_filename.pkcs12> -name "IFMAP Client"`
5. Type the following command to copy the pkcs12 file to the /opt/qradar/conf/key_certificates directory:`cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates`
6. Create a client on the IF-MAP server with the Certificate authentication and upload the SSL certificate. For assistance, contact your IF-MAP server administrator.

7. Change the permissions of the directory by typing the following commands:`chmod 755 /opt/qradar/conf/trusted_certificateschmod 644 /opt/qradar/conf/trusted_certificates/*.cert`
8. Type the following command to restart the Tomcat service:`service tomcat restart`

Data retention

Configure custom retention periods for specific data.

Retention buckets define retention policies for events and flows that match custom filter requirements. As QRadar receives events and flows, each event and flow is compared against retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the retention policy time period is reached. This feature enables you to configure multiple retention buckets.

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

Configuring retention buckets

By default, the Event Retention and Flow Retention windows provide a default retention bucket and 10 unconfigured retention buckets. Until you configure a retention bucket, all events or flows are stored in the default retention bucket.

About this task

The Event Retention and Flow Retention windows provide the following information for each retention bucket:

Table 23. Retention window parameters

Parameter	Description
Order	The priority order of the retention buckets.
Name	The name of the retention bucket.
Retention	The retention period of the retention bucket.
Compression	The compression policy of the retention bucket.
Deletion Policy	The deletion policy of the retention bucket.
Filters	The filters applied to the retention bucket. Move your mouse pointer over the **Filters** parameter for more information on the applied filters.
Distribution	The retention bucket usage as a percentage of total data retention in all your retention buckets.
Enabled	Specifies if the retention bucket is enabled (true) or disabled (false).

Table 23. Retention window parameters (continued)

Parameter	Description
Creation Date	The date and time the retention bucket was created.
Modification Date	The date and time the retention bucket was last modified.

The toolbar provides the following functions:

Table 24. Retention window toolbar

Function	Description
Edit	Edit a retention bucket.
Enable/Disable	Enable or disable a retention bucket. When you disable a bucket, any new data that matches the requirements for the disabled bucket are stored in the next bucket that matches the properties.
Delete	Delete a retention bucket. When you delete a retention bucket, the data contained in the retention bucket is not removed from the system, only the criteria defining the bucket is deleted. All data is maintained in storage.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources** .
3. Click the **Event Retention** or **Flow Retention** icon.
4. Double-click the first available retention bucket.
5. Configure the following parameters:

Parameter	*Description*
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	Select a retention period. When the retention period is reached, data is deleted according to the *Delete data in this bucket* parameter.
Allow data in this bucket to be compressed	Select the check box to enable data compression, and then select a time frame from the list box. When the time frame is reached, all data in the retention bucket are eligible to be compressed. This increases system performance by guaranteeing that no data is compressed within the specified time period. Compression only occurs when used disk space reaches 83% for payloads and 85% for records.

Parameter	*Description*
Delete data in this bucket	Select a deletion policy. Select **When storage space is required** if you want data that matches the *Keep data placed in this bucket for* parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. Select **Immediately after the retention period has expired** if you want data to be deleted immediately on matching the **Keep data placed in this bucket for** parameter. The data is deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements. When storage is required, only data that matches the **Keep data placed in this bucket for** parameter are deleted.
Description	Type a description for the retention bucket.
Current Filters	Configure your filters. From the first list, select a parameter you want to filter for. For example, Device, Source Port, or Event Name. From the second list, select the modifier you want to use for the filter. The list of modifiers depends on the attribute selected in the first list. In the text field, type specific information related to your filter and then click **Add Filter**. The filters are displayed in the **Current Filters** text box. You can select a filter and click **Remove Filter** to remove a filter from the **Current Filter** text box.

6. Click **Save**.
7. Click **Save** again.

   Your retention bucket starts storing data that match the retention parameters immediately.

Managing retention bucket sequence

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

About this task

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

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Event Retention** or **Flow Retention** icon.
4. Click the icon.
5. Select and move the required retention bucket to the correct location.

Editing a retention bucket

If required, you can edit the parameters of a retention bucket.

About this task

On the Retention Parameters window, the Current Filters pane is not displayed when editing a default retention bucket.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Choose one of the following options:
4. Click the **Event Retention** icon.
5. Click the **Flow Retention** icon.
6. Select the retention bucket you want to edit, and then click **Edit**.
7. Edit the parameters. For more information see, "Configuring retention buckets" on page 74.
8. Click **Save**.

Enabling and disabling a retention bucket

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

About this task

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Choose one of the following options:
4. Click the **Event Retention** icon.

5. Click the **Flow Retention** icon.
6. Select the retention bucket you want to disable, and then click **Enable/Disable**.

Deleting a Retention Bucket

When you delete a retention bucket, the events or flows contained in the retention bucket are not removed from the system, only the criteria defining the bucket is deleted. All events or flows are maintained in storage.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Choose one of the following options:
4. Click the **Event Retention** icon.
5. Click the **Flow Retention** icon.
6. Select the retention bucket you want to delete, and then click **Delete**.

Configuring system notifications

You can configure system performance alerts for thresholds. This section provides information about configuring your system thresholds.

About this task

The following table describes the Global System Notifications window parameters

Table 25. Global System Notifications window parameters

Parameter	Description
System load over 1 minute	Type the threshold system load average over the last minute.
System load over 5 minutes	Type the threshold system load average over the last 5 minutes.
System load over 15 minutes	Type the threshold system load average over the last 15 minutes.
Percentage of swap used	Type the threshold percentage of used swap space.
Received packets per second	Type the threshold number of packets received per second.
Transmitted packets per second	Type the threshold number of packets transmitted per second.
Received bytes per second	Type the threshold number of bytes received per second.
Transmitted bytes per second	Type the threshold number of bytes transmitted per second.
Receive errors	Type the threshold number of corrupted packets received per second.
Transmit errors	Type the threshold number of corrupted packets transmitted per second.
Packet collisions	Type the threshold number of collisions that occur per second while transmitting packets.

Table 25. Global System Notifications window parameters (continued)

Parameter	Description
Dropped receive packets	Type the threshold number of received packets that are dropped per second due to a lack of space in the buffers.
Dropped transmit packets	Type the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers.
Transmit carrier errors	Type the threshold number of carrier errors that occur per second while transmitting packets.
Receive frame errors	Type the threshold number of frame alignment errors that occur per second on received packets.
Receive fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets.
Transmit fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Global System Notifications** icon.
4. Enter values for each parameter that you want to configure.
5. For each parameter, select **Enabled** and **Respond if value is** and then select one of the following options:

Option	Description
Greater Than	An alert occurs if the parameter value exceeds the configured value.
Less Than	An alert occurs if the parameter value is less than the configured value.

6. Type a description of the preferred resolution to the alert.
7. Click **Save**.
8. On the tab menu, click **Deploy Changes**.

Configuring the Console settings

The Console provides real-time views, reports, alerts, and in-depth investigation of network traffic and security threats. You can configure the Console to manage distributed QRadar deployments.

About this task

The following table describes the Console settings:

Table 26. Console settings

Settings	Description
Console Settings	
ARP - Safe Interfaces	Type the interfaces that you want to be excluded from ARP resolution activities.
Results Per Page	Type the maximum number of results you want to display on the user interface. This parameter applies to the **Offenses**, **Log Activity**, **Assets**,**Network Activity**, and **Reports** tabs. For example, if the **Default Page Size** parameter is configured to 50, the **Offenses** tab displays a maximum of 50 offenses.
Authentication Settings	
Persistent Session Timeout (in days)	Type the length of time, in days, that a user system is persisted.
Maximum Login Failures	Type the number of times a login attempt can fail.
Login Failure Attempt Window (in minutes)	Type the length of time during which a maximum number of login failures can occur before the system is locked.
Login Failure Block Time (in minutes)	Type the length of time that the system is locked if the maximum login failures value is exceeded.
Login Host Whitelist	Type a list of hosts who are exempt from being locked out of the system. Enter multiple entries using a comma-separated list.
Inactivity Timeout (in minutes)	Type the amount of time that a user is automatically logged out of the system if no activity occurs.
Login Message File	Type the location and name of a file that includes content you want to display on the QRadar login window. The contents of the file are displayed below the current login window. The login message file must be located in the `/opt/qradar/conf` directory on your system. This file will be in text format.

Table 26. Console settings (continued)

Settings	Description
Event Permission Precedence	From the list box, select the level of network permissions you want to assign to users. This parameter affects the events that are displayed on the **Log Activity** tab. The options include: • **Network Only** - A user must have access to either the source network or the destination network of the event to have that event display on the **Log Activity** tab. • **Devices Only** - A user must have access to either the device or device group that created the event to have that event display on the **Log Activity** tab. • **Networks and Devices** - A user must have access to both the source or the destination network and the device or device group to have an event display on the **Log Activity** tab. • **None** - All events are displayed on the **Log Activity** tab. Any user with Log Activity role permissions is able to view all events. For more information about managing users, see Chapter 2, "User management," on page 7.
DNS Settings	
Enable DNS Lookups for Asset Profiles	From the list box, select whether you want to enable or disable the ability for QRadar to search for DNS information in asset profiles. When enabled, this information is available in the right-click menu for the IP address or host name that is located in the **Host Name (DNS Name)** field in the asset profile.
Enable DNS Lookups for Host Identity	From the list box, select whether you want to enable or disable the ability for QRadar to search for host identity information. When enabled, this information is available in the right-click menu for any IP address or asset name.
WINS Settings	
WINS Server	Type the location of the Windows Internet Naming Server (WINS) server.
Reporting Settings	
Report Retention Period	Type the period, in days, that you want the system to maintain reports.
Data Export Settings	
Include Header in CSV Exports	From the list box, select whether you want to include a header in a CSV export file.
Maximum Simultaneous Exports	Type the maximum number of exports you want to occur at one time.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Console** icon.
4. Enter values for the parameters.
5. Click **Save**.
6. On the **Admin** tab menu, click **Deploy Changes**.

Custom offense close reasons

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

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

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

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

Adding a custom offense close reason

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

About this task

The Custom Offense Close Reasons window provides the following parameters.

Table 27. Custom Close Reasons window parameters

Parameter	Description
Reason	The reason that is displayed in the **Reason for Closing** list box on the Close Offense window of the **Offenses** tab.
Created by	The user that created this custom offense close reason.
Date Created	The date and time of when the user created this custom offense close reason.

Procedure

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

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

Editing custom offense close reason

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

Procedure

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

Deleting a custom offense close reason

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

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Custom Offense Close Reasons** icon.
4. Select the reason you want to delete.
5. Click **Delete**.
6. Click **OK**.

Index management

The Index Management feature allows you to control database indexing on event and flow properties.

Indexing event and flow properties allows you to optimize your searches. You can enable indexing on any property that is listed in the Index Management window and you can enable indexing on more than one property.

The Index Management feature also provides statistics, such as:

- The percentage of saved searches running in your deployment that include the indexed property
- The volume of data that is written to the disk by the index during the selected time frame

To enable payload indexing, you must enable indexing on the Quick Filter property. For more information on payload indexing, see the *Enable Payload Indexing for Quick Filtering Technical Note*.

Enabling indexes

The Index Management window lists all event and flow properties that can be indexed and provides statistics for the properties. Toolbar options allow you to enable and disable indexing on selected event and flow properties.

About this task

About this task

Modifying database indexing might decrease system performance, therefore, we recommend that you monitor the statistics after enabling indexing on multiple properties.

The Index Management window provides the following parameters.

Table 28. Index Management window parameters

Parameter	Description
Display	Displays the time range used to calculate the statistics for each property. From the list box, you can select a new time range. After you select a new time range option, the statistics are refreshed.
View	Allows you to display properties filtered on the *Indexed* parameter.
Database	Allows you to display properties filtered on the *Database* parameter.
Show	Allows you to display all properties or only custom properties. Options include: • *All* - Displays all properties in the Index Management list. • *Custom* - Displays only custom event and flow properties. Custom properties are properties that you can create by extracting from unnormalized data using RegEx statements or calculated properties that are created by performing operations on existing properties. For more information on custom properties, see the *IBM Security QRadar SIEM Users Guide* .
Indexed	Indicates whether the property is indexed or not:
Property	Displays the name of the property.
% of Searches Using Property	Displays the percentage of searches that include this property that have performed in the specified time range.
% of Searches Hitting Index	Displays the percentage of searches that include this property that have performed in the specified time range and successfully used the index.

Table 28. Index Management window parameters (continued)

Parameter	Description
% of Searches Missing Index	Displays the percentage of searches that include this property that have performed in the specified time range and did not use the index.
Data Written	Displays the volume of data written to the disk by the index in the time range specified in the *Display* list box.
Database	Displays the name of the database the property is stored in. Databases include:

The Index Management toolbar provides the following options:

Table 29. Index Management window parameters

Option	Description
Enable Index	Select one or more properties in the Index Management list, and then click this icon to enable indexing on the selected parameters.
Disable Index	Select one or more properties in the Index Management list, and then click this icon to disable indexing on the selected parameters.
Quick Search	Type your keyword in the *Quick Search* field and click the *Quick Filter* icon or press Enter on the keyboard. All properties that match your keyword are displayed in the Index Management list.

Click the *Admin* tab.

Procedure

1. On the navigation menu, click *System Configuration* .
2. Click the *Index Management* icon.
3. Select one or more properties from the Index Management list.
4. Choose one of the following options:
   - Click *Enable Index*.
   - Click *Disable Index*.
5. Click *Save* .
6. Click *OK* .

Results

In lists that include event and flow properties, indexed property names are appended with the following text: *[Indexed]* . Examples of such lists include the search parameters on the *Log Activity* and *Network Activity* tab search criteria pages and the Add Filter window.

Chapter 6. Reference sets management

Using the Reference Set Management window, you can create and manage reference sets. You can also import elements into a reference set from an external file.

A reference set is a set of elements that are derived from events and flows that occur on your network. Examples of elements that are derived from events are IP addresses or user names.

After you create a reference set, you can create rules to detect log activity or network activity that is associated with the reference set. For example, you can create a rule to detect when an unauthorized user attempts to access your network resources. You can also configure a rule to add an element to a reference set when log activity or network activity matches the rule conditions. For example, you can create a rule to detect when an employee accesses a prohibited website and add that employee's IP address to a reference set. For more information on configuring rules, see the *Users Guide* for your product.

Adding a reference set

From the **Admin** tab, you can add a reference set that you can include in rule tests.

About this task

After you create a reference set, the reference set is listed on the Reference Set Management window. In the Rule wizard, this reference set is listed as an option on the **Rule Response** page. After you configure one or more rules to send elements to this reference set, the **Number of Elements**, **Associated Rules**, and **Capacity** parameters are automatically updated.

Procedure

1. On the Reference Set Management window, click **New**.
2. Configure the parameters:

Table 30. Reference Set parameters

Parameter	Description
Name	A unique name for this reference set.
Type	You cannot edit the **Type** parameter after you create a reference set.
Time to Live of Elements	The amount of time that you want to maintain each element in the reference set. If you specify an amount of time, you must also indicate when you want to start tracking time for an element.

3. Click **Create**.

Editing a reference set

Use the Reference Set Management window to edit a reference set.

Procedure

1. In the **Reference Set Management** window, select a reference set
2. Click **Edit**.
3. Edit the parameters.

Table 31. Reference Set parameters

Parameter	Description
Name	A unique name for this reference set. The maximum length is 255 characters
Type	You cannot edit the **Type** parameter after you create a reference set.
Time to Live of Elements	The amount of time that you want to maintain each element in the reference set. If you specify an amount of time, you must also indicate when you want to start tracking time for an element. **Lives Forever** is the default setting.

4. Click **Submit**.

Deleting reference sets

You can delete a reference set from the Reference Set Management window.

About this task

When you delete reference sets, a confirmation window indicates whether the reference sets that you want to delete have rules that are associated with them. After you delete a reference set, the **Add to Reference Set** configuration is cleared from the associated rules.

Tip: Before you delete a reference set, you can view associated rules in the **Reference** tab.

Procedure

Choose one of the following options:

- On the Reference Set Management window, select a reference set, and then click **Delete**.
- On the Reference Set Management window, use the **Quick Search** text box to display only the reference sets that you want to delete, and then click **Delete Listed**.

Viewing the contents of a reference set

The **Content** tab provides a list of the elements that are included in this reference set.

Procedure

1. On the Reference Set Management window, select a reference set.
2. Click **View Contents**.

3. To view contents, click the **Content** tab.

   Tip: Use the **Quick Search** field to filter for specific elements. All elements that match the keyword are listed in the **Content** list. Then, you can select the action from the toolbar.

Table 32. Content tab parameters

Parameter	Description
Value	The value of the element. For example, if the reference contains a list of IP addresses, the value is the IP address.
Origin	The ***rulename*** is placed in the reference set as a response to a rule. The **User** is imported from an external file or manually added to the reference set.
Time to Live	The time that is remaining until this element is removed from the reference set.
Date Last Seen	The date and time that this element was last detected on your network.

4. Click the **References** tab and view the references.

   Tip: Use the **Quick Search** field to filter for specific elements. All elements that match the keyword are listed in the **Content** list. Then, you can select the action from the toolbar.

Table 33. Content tab parameters

Parameter	Description
Rule Name	The name of this rule.
Group	The name of the group this rule belongs to.
Category	The category of the rule. Options include **Custom Rule** or **Anomaly Detection Rule**.
Type	The type of this rule.
Enabled	Indicates whether the rule is enabled or disabled.
Response	The responses that are configured for this rule.
Origin	**System** indicates a default rule. **Modified** indicates that a default rule was customized. **User** indicates a user-created rule.

5. To view or edit an associated rule, double-click the rule in the **References** list.
   In the Rule wizard, you can edit the rule configuration settings.

Adding an element to a reference set

You add an element to a reference set by using the Reference Set Management window.

Procedure

1. On the Reference Set Management window, select a reference set.
2. Click **View Contents**.
3. Click the **Content** tab.
4. On the toolbar, click **New**.
5. Configure the following parameters:

Parameter	Description
Value(s)	If you want to type multiple values, include a separator character between each value, and then specify the separator character in the **Separator Character** field.
Separator Character	Type the separator character that you used in the **Value(s)** field.

6. Click **Add**.

Deleting elements from a reference set

You can delete elements from a reference set.

Procedure

1. On the Reference Set Management window, select a reference set.
2. Click **View Contents**.
3. Click the **Content** tab.
4. Choose one of the following options:
   - Select an element, and then click **Delete**.
   - Use the **Quick Search** text box to display only the elements that you want to delete, and then click **Delete Listed**.
5. Click **Delete**.

Importing elements into a reference set

You can import elements from an external CSV or text file.

Before you begin

Ensure that the CSV or text file that you want to import is stored on your local desktop.

Procedure

1. On the Reference Set Management window, select a reference set.
2. Click **View Contents**.
3. Click the **Content** tab.
4. On the toolbar, click **Import**.
5. Click **Browse**.
6. Select the CSV or text file that you want to import.
7. Click **Import**.

Exporting elements from a reference set

You can export reference set elements to an external CSV or text file.

Procedure

1. On the Reference Set Management window, select a reference set.
2. Click **View Contents**.
3. Click the **Content** tab.
4. On the toolbar, click **Export**.
5. Choose one of the following options:
6. If you want to open the list for immediate viewing, select the **Open with** option and select an application from the list box.
7. If you want to save the list, select the **Save File** option.
8. Click **OK**.

Chapter 7. Reference data collections

Use the `ReferenceDataUtil.sh` utility to make complex reference data collections. Use reference data collections to store, retrieve, and test complex data structures.

You can create the following reference data collection types:

Reference map
Data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the **Username** parameter as a key and the user's **Global ID** as a value.

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

Reference map of maps
Data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you can create a map of maps. Use the **Source IP** parameter as the first key, the **Application** parameter as the second key, and the **Total Bytes** parameter as the value.

Reference table
In a reference table, data is stored in a table that maps one key to another key, which is then mapped to single value. The second key has a assigned type. This mapping is similar to a database table where each column in the table is associated with a type.

CSV file requirements for reference data collections

If you plan to import an external file containing data elements into a reference data collection, ensure that the file is in Comma Separated Value (CSV) format. Also, ensure that you copied the CSV file to your system.

The CSV file must follow the format in the examples reference data collections. The # symbol in the first column indicates a comment line. The first non-comment line is the column header and identifies the column name (ie., `key1, key2, data`). Then each non-commented line that follows is a data record that is added to the map. Keys are alphanumeric strings.

Example 1: Reference map

```
#
#
# ReferenceMap
#
key1,data
key1,value1
key2,value2
```

Example 2: Reference map of sets

```
#
#
# ReferenceMapOfSets
#
key1,data
key1,value1
key1,value2
```

Example 3: Reference map of maps

```
#
#
# ReferenceMapOfMaps
#
key1,key2,data
map1,key1,value1
map1,key2,value2
```

Example 3: Reference table

```
#
#
# ReferenceTable
#
key1,key2,type,data
map1,key1,type1,value1
map1,key2,type 1,value2
```

Creating a reference data collection

Use the `ReferenceDataUtil.sh` utility to create a reference data collection.

Procedure

1. Using SSH, log in to QRadar as the root user.
2. Go to the /opt/qradar/bin directory.
3. To create the reference data collection, type the following command:

   `./ReferenceDataUtil.sh create` *`name count`* `[MAP | MAPOFSETS | MAPOFMAPS | REFTABLE] [ALN | NUM | IP | PORT | ALNIC | DATE] [TIMEOUT_TYPE] [TIMETOLIVE]`
4. To populate the map with data from an external file, type the following command:

   `./ReferenceDataUtil.sh load` *`name filename`* `[-encoding=...] [-sdf=" ... "]`

What to do next

Log in to the user interface to create rules that add data to your reference data collections. You can also create rule tests that detect activity from elements that are in your reference data collection. For more information about creating rules and rule tests, see the *Users Guide* for your product.

ReferenceDataUtil.sh command reference

You can manage your reference data collections using the `ReferenceDataUtil.sh` utility.

create

Creates a reference data collection.

name
The name of the reference data collection.

[MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
The type of reference data collection.

[ALN | ALNIC | NUM | IP | PORT | DATE]
The type of data in the reference set:

- **ALN** specifies a reference data collection of alphanumeric values. This data type supports IPv4 and IPv6 addresses.
- **ALNIC** specifies a reference data collection of alphanumeric values but tests ignore the case. This data type supports IPv4 and IPv6 addresses.
- **NUM** specifies a reference data collection of numeric values.
- **IP** specifies a reference data collection of IP addresses. This data type supports only IPv4 address.
- **PORT** specifies a reference data collection of PORT addresses.
- **DATE** specifies a reference data collection of DATE values.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Specifies whether the amount of time the data elements remain in the reference data collection is from the time the element was first seen or last seen.

[-TimeToLive='']
The amount of time the data elements remain in the reference data collection.

[-keyType=name:elementType,name:elementType,...]
A mandatory **REFTABLE** parameter of consisting of key name to **ELEMENTTYPE** pairs.

[-key1Label='']
An optional label for key1.

[-valueLabel='']
An optional label for the values of the collection.

update

Updates a reference data collection.

name
The name of the reference data collection.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Specifies whether the amount of time the data elements remain in the reference data collection is from the time the element was first seen or last seen.

[-timeToLive='']
The amount of time the data elements remain in the reference data collection.

[-keyType=name:elementType,name:elementType,...]
A mandatory **REFTABLE** parameter of consisting of key name to **elementType** pairs.

[-key1Label='']
An optional label for key1.

[-valueLabel='']
An optional label for the values of the collection.

add

Adds a data element to a reference data collection

name
The name of the reference data collection.

<value> <key1> [key2]
The key value pair that you want to add. MAP and MAPOFSETS require Key 1. MAPOFMAPS and REFTABLE require Key 1 and Key 2. Keys are alphanumeric strings.

[-sdf=" ... "]
The Simple Date Format string that is used to parse the date data.

delete

Deletes an element from a reference data collection.

name
The name of the reference data collection.

<value> <key1> [key2]
The key value pair that you want to delete. MAP and MAPOFSETS require Key 1. MAPOFMAPS and REFTABLE require Key 1 and Key 2. Keys are alphanumeric strings.

[-sdf=" ... "]
The Simple Date Format string that is used to parse the date data.

remove

Removes a reference data collection.

name
The name of the reference data collection.

purge

Purges all elements from a reference data collection.

name
The name of the reference data collection.

list

Lists elements in a reference data collection.

name
The name of the reference data collection.

[displayContents]
Lists all elements in the specified reference data collection.

listall

Lists all elements in all reference data collection.

[displayContents]
Lists all elements in all reference data collections.

load

Populates a reference data collections with data from an external CSV file.

name
The name of the reference data collection.

filename
The fully qualified file name to be loaded. Each line in the file represents a record to be added to the reference data collection.

[-encoding=...]
Encoding that is used to read the file.

[-sdf=" ... "]
The Simple Date Format string that is used to parse the date data.

Chapter 8. Managing authorized services

You can configure authorized services on the **Admin** tab to pre-authenticate a customer support service for your QRadar deployment.

Authenticating a customer support service allows the service to connect to your QRadar user interface and either dismiss or update notes to an offense using a web service. You can add or revoke an authorized service at any time.

The Manage Authorized Services window provides the following information:

Table 34. Parameters for authorized services

Parameter	Description
Service Name	The name of the authorized service.
Authorized By	The name of the user or administrator that authorized the addition of the service.
Authentication Token	The token that is associated with this authorized service.
User Role	The user role that is associated with this authorized service.
Created	The date that this authorized service was created.
Expires	The date and time that the authorized service expires. By default, the authorized service is valid for 30 days.

Viewing authorized services

The Authorized Services window displays a list of authorized services, from which you can copy the token for the service.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Authorized Services**.
4. From the Manage Authorized Services window, select the appropriate authorized service.

   The token is displayed in the **Selected Token** field in the top bar. You can copy the token into your vendor software to authenticate with QRadar.

Adding an authorized service

Use the Add Authorized Service window to add a new authorized service.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Authorized Services**.

4. Click **Add Authorized Service**.
5. In the **Service Name** field, type a name for this authorized service. The name can be up to 255 characters in length.
6. From the **User Role** list, select the user role that you want to assign to this authorized service. The user roles that are assigned to an authorized service determine the functions that this service can access on the QRadar user interface.
7. In the **Expiry Date** list, type or select a date that you want this service to expire. If an expiry date is not required, select **No Expiry**
8. Click **Create Service**.

   The confirmation message contains a token field that you must copy into your vendor software to authenticate with QRadar SIEM.

Revoking authorized services

Use the Add Authorized Service window to revoke an authorized service.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Authorized Services**.
4. From the Manage Authorized Services window, select the service that you want to revoke.
5. Click **Revoke Authorization**.

Customer support authenticated service

After you configure an authorized service, you must configure your customer support service to access QRadar offense information.

For example, you can configure QRadar to send an SNMP trap that includes the offense ID information.

Your service uses an authorized token to authenticate to QRadar by passing the information through an HTTP query string. When authenticated, the service interprets the authentication token as the user name during the session.

Your customer support service must use a query string to update notes, dismiss, or close an offense.

Dismiss an offense

Your customer support service must use a query string to dismiss an offense.

To dismiss an offense, your customer support service must use the following query string:

```
https://<IP address >/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId= OffenseList
&nextForward=offensesearch&attribute=dismiss&daoName =offense&value=1
&authenticationToken=<Token>
```

Table 35. Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your QRadar system.
<Offense ID>	The identifier that is assigned to the QRadar offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide*.
<Token>	The token identifier that is provided to the authorized service on the QRadar user interface.

Close an offense

Your customer support service must use a query string to close an offense.

To close an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&id=<Offense ID>&nextPageId= OffenseList
&nextForward=offensesearch&attribute=dismiss&daoName =offense&value=2
&authenticationToken=<Token>
```

Table 36. Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your QRadar system.
<Offense ID>	The identifier that is assigned to the QRadar offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide*.
<Token>	The token identifier that is provided to the authorized service on the QRadar user interface.

Add notes to an offense

You must use a query string to add notes to an offense.

To add notes to an offense, your customer support service must use the following query string:

```
https://<IP Address>/console/do/sem/properties?appName=Sem&amp;
dispatch=updateProperties&amp;id=<Offense ID>&amp;nextPageId=
OffenseList&amp;nextForward=offensesearch&amp;attribute=notes&amp;daoName
=offense&amp;value=<NOTES>&amp;authenticationToken=<Token>
```

Table 37. Query string parameters for the customer support service

Parameter	Description
<IP address>	The IP address of your QRadar system.
<Offense ID>	The identifier that is assigned to the QRadar offense. To obtain the offense ID, see the **Offenses** tab. For more information, see the *IBM Security QRadar SIEM Users Guide*.

Table 37. Query string parameters for the customer support service (continued)

Parameter	Description
<Token>	The token identifier that is provided to the authorized service on the QRadar user interface.

Chapter 9. Manage backup and recovery

You can back up and recover QRadar configuration information and data.

You can use the backup and recovery feature to back up your event and flow data; however, you must restore event and flow data manually. For assistance in restoring your event and flow data, see the *Restoring Your Data Technical Note*.

By default, QRadar creates a backup archive of your configuration information daily at midnight. The backup archive includes configuration information, data, or both from the previous day.

You can use two types of backups; configuration backups and data backups.

Configuration backups include the following components:

- Assets
- Certificates
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Flow sources
- Flow and event searches
- Groups
- Index management information
- License key information
- Log sources
- Offenses
- Store and Forward schedules
- User and user roles information
- Vulnerability data (if QRadar Vulnerability Manager is installed)

Data backups include the following information:

- Audit log information
- Event data
- Flow data
- Report data
- Indexes
- Reference set elements

Backup archive management

View and manage backup archives

From the Backup Management Archive window, you can view and manage all successful backup archives.

Viewing backup archives

Use the Backup Archives window to view a list of your backup archives.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Backup and Recovery**.

Importing a backup archive

Importing a backup archive is useful if you want to restore a backup archive that was created on another QRadar host.

About this task

If you place a QRadar backup archive file in the `/store/backupHost/inbound` directory on the Console server, the backup archive file is automatically imported.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Backup and Recovery** icon.
4. In the **Upload Archive** field, click **Browse**.
5. Locate and select the archive file that you want to upload. The archive file must include a .tgz extension.
6. Click **Open**.
7. Click **Upload**.

Deleting a backup archive

To delete a backup archive file, the backup archive file and the Host Context component must be located on the same system. The system must also be in communication with the Console and no other backup can be in progress.

About this task

If a backup file is deleted, it is removed from the disk and from the database. Also, the entry is removed from this list and an audit event is generated to indicate the removal.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Backup and Recovery**.
4. In the **Existing Backups** section, select the archive that you want to delete.
5. Click **Delete**.

Backup archive creation

By default, QRadar creates a backup archive of your configuration information daily at midnight. The backup archive includes your configuration information, data, or both from the previous day. You can customize this nightly backup and create an on-demand configuration backup, as required.

Scheduling nightly backup

Use the Backup Recovery Configuration window to configure a night scheduled backup process.

About this task

By default, the nightly backup process includes only your configuration files. You can customize your nightly backup process to include data from your Console and selected managed hosts. You can also customize your backup retention period, backup archive location, the time limit for a backup to process before timing out, and the backup priority in relation to other QRadar processes.

The Backup Recovery Configuration window provides the following parameters:

Table 38. Backup Recovery Configuration parameters

Parameter	Description
General Backup Configuration	
Backup Repository Path	Type the location where you want to store your backup file. The default location is `/store/backup`. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts. If you modify this path, make sure the new path is valid on every system in your deployment. • Active data is stored on the `/store` directory. If you have both active data and backup archives stored in the same directory, data storage capacity might easily be reached and your scheduled backups might fail. We recommend you specify a storage location on another system or copy your backup archives to another system after the backup process is complete. You can use a Network File System (NFS) storage solution in your QRadar deployment. For more information on using NFS, see the *Offboard Storage Guide*.
Backup Retention Period (days)	Type or select the length of time, in days, that you want to store backup files. The default is 2 days. This period of time only affects backup files generated as a result of a scheduled process. On-demand backups or imported backup files are not affected by this value.
Nightly Backup Schedule	Select a backup option.

Table 38. Backup Recovery Configuration parameters (continued)

Parameter	Description
Select the managed hosts you would like to run data backups:	This option is only displayed if you select the **Configuration and Data Backups** option. All hosts in your deployment are listed. The first host in the list is your Console; it is enabled for data backup by default, therefore no check box is displayed. If you have managed hosts in your deployment, the managed hosts are listed below the Console and each managed host includes a check box. Select the check box for the managed hosts you want to run data backups on. For each host (Console or managed hosts), you can optionally clear the data items you want to exclude from the backup archive.
Configuration Only Backup	
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 180 minutes. If the backup process exceeds the configured time limit, the backup process is automatically canceled.
Backup Priority	From this list box, select the level of importance that you want the system to place on the configuration backup process compared to other processes. A priority of medium or high have a greater impact on system performance.
Data Backup	
Backup Time Limit (min)	Type or select the length of time, in minutes, that you want to allow the backup to run. The default is 1020 minutes. If the backup process exceeds the configured time limit, the backup is automatically canceled.
Backup Priority	From the list, select the level of importance you want the system to place on the data backup process compared to other processes. A priority of medium or high have a greater impact on system performance.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Backup and Recovery**.
4. On the toolbar, click **Configure**.

5. On the Backup Recovery Configuration window, customize your nightly backup.
6. Click **Save**.
7. Close the Backup Archives window.
8. On the **Admin** tab menu, click **Deploy Changes**.

Creating an on-demand configuration backup archive

If you must back up your configuration files at a time other than your nightly scheduled backup, you can create an on-demand backup archive. On-demand backup archives include only configuration information.

About this task

You initiate an on-demand backup archive during a period when QRadar has low processing load, such as after normal office hours. During the backup process, system performance is affected.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **Backup and Recovery**.
4. From the toolbar, click **On Demand Backup**.
5. Enter values for the following parameters:

Option	Description
Name	Type a unique name that you want to assign to this backup archive. The name can be up to 100 alphanumeric characters in length. The name can contain following characters: underscore (_), dash (-), or period (.).
Description	Type a description for this configuration backup archive. The description can be up to 255 characters in length.

6. Click **Run Backup**.

   You can start a new backup or restore processes only after the on-demand backup is complete. You can monitor the backup archive process in the Backup Archives window. See "Viewing backup archives" on page 104.

Backup archive restoration

Restoring a backup archive is useful if you want to restore previously archived configuration files, asset data, and offense data on yourQRadar system.

Before you restore a backup archive, note the following considerations:

- You can only restore a backup archive created within the same release of software, including the patch level. For example, if you are running IBM Security QRadar 7.1.0 (MR2), the backup archive must have been created in IBM Security QRadar.
- The restore process only restores your configuration information, asset data, and offense data. For assistance in restoring your event or flow data, see the *Restoring Your Data Technical Note* .

- If the backup archive originated on a NATed Console system, you can only restore that backup archive on a NATed system.

During the restore process, the following steps are taken on the Console:

1. Existing files and database tables are backed up.
2. Tomcat is shut down.
3. All system processes are shut down.
4. Files are extracted from the backup archive and restored to disk.
5. Database tables are restored.
6. All system processes are restarted.
7. Tomcat restarts.

Restoring a backup archive

You can restore a backup archive. Restoring a backup archive is useful if you have a system hardware failure or you want to store a backup archive on a replacement appliance.

About this task

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

A window provides the status of the restore process. This window provides any errors for each host and instructions for resolving the errors.

The following parameters are available in the Restore a Backup window:

Table 39. Restore a Backup parameters

Parameter	Description
Name	The name of the backup archive.
Description	The description, if any, of the backup archive.
Type	The type of backup. Only configuration backups can be restored, therefore, this parameter displays **config**.
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive.
Restore Configuration	Lists the configuration items to include in the restoration of the backup archive. To remove items, you can clear the check boxes for each item you want to remove or clear the **Select All Configuration Items** check box.
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive.

Table 39. Restore a Backup parameters (continued)

Parameter	Description
Restore Data	Lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Backup and Recovery**.
4. Select the archive that you want to restore.
5. Click **Restore**.
6. On the Restore a Backup window, configure the parameters.
7. Click **Restore**.
8. Click **OK**.
9. Click **OK**.
10. Choose one of the following options:
    - If the user interface was closed during the restore process, open a web browser and log in to QRadar.
    - If the user interface was not closed, the login window is displayed. Log in to QRadar.
11. Follow the instructions on the status window.

What to do next

After you verify that your data is restored to your system, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after a backup, the secondary host displays a failed status on the System and License Management window.

Restoring a backup archive created on a different QRadar system

Each backup archive includes the IP address information of the system from which the backup archive was created. When you restore a backup archive from a different QRadar system, the IP address of the backup archive and the system that you are restoring are mismatched. You can correct the mismatched IP addresses.

About this task

You can restart the Console only after the restore process is complete.

The restore process can take up to several hours; the process time depends on the size of the backup archive that must be restored. When complete, a confirmation message is displayed.

A window provides the status of the restore process. This window provides any errors for each host and instructions for resolving the errors.

You must stop the iptables service on each managed host in your deployment. The Iptables service is a Linux based firewall.

The Restore a Backup (Managed Hosts Accessibility) window provides the following information.

Table 40. Restore a Backup (Managed Host Accessibility) parameters

Parameter	Description
Host Name	The managed host name.
IP Address	The IP address of the managed host.
Access Status	The access status to the managed host.

The Restore a Backup window provides the following parameters:

Table 41. Restore a Backup parameters

Parameter	Description
Name	The name of the backup archive.
Description	The description, if any, of the backup archive.
Type	The type of backup. Only configuration backups can be restored, therefore, this parameter displays**config**.
Select All Configuration Items	When selected, this option indicates that all configuration items are included in the restoration of the backup archive. This check box is selected by default. To clear all configuration items, clear the check box.
Restore Configuration	Lists the configuration items to include in the restoration of the backup archive. All items are selected by default. To remove items, you can clear the check boxes for each item you want to remove or clear the **Select All Configuration Items** check box.
Select All Data Items	When selected, this option indicates that all data items are included in the restoration of the backup archive. This check box is selected by default. To clear all data items, clear this check box.
Restore Data	Lists the configuration items to include in the restoration of the backup archive. All items are cleared by default. To restore data items, you can select the check boxes for each item you want to restore.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Backup and Recovery**.
4. Select the archive that you want to restore.

5. Click **Restore**.
6. On the Restore a Backup window, configure the parameters.
7. Click **Restore**.
8. Stop the IP tables:
   a. Using SSH, log in to the managed host as the root user.
   b. Type the command, **service iptables stop**.
   c. Repeat for all managed hosts in your deployment.
9. On the Restore a Backup window, click **Test Hosts Access**.
10. After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**.
11. If the **Access Status** column indicates a status of **No Access** for a host, stop iptables again, and then click **Test Host Access** again to attempt a connection.
12. On the Restore a Backup window, configure the parameters.
13. Click **Restore**.
14. Click **OK**.
15. Click **OK** to log in.
16. Choose one of the following options:
    - If the user interface was closed during the restore process, open a web browser and log in to QRadar.
    - If the user interface was not closed, the login window is displayed. Log in to QRadar.
17. View the results of the restore process and follow the instructions to resolve any errors.
18. Refresh your web browser window.
19. From the **Admin** tab, select **Advanced Deploy Full Configuration**.

What to do next

After you verify that your data is restored to your system, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, or log source protocols.

If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data after the system is restored. If the secondary host was removed from the deployment after a backup, the secondary host displays a failed status on the System and License Management window.

Restoring data

You can restore the data on your QRadar Console and managed hosts from backup files. The data portion of the backup files includes information about all offenses, including source and destination IP address information, asset data, event category information, vulnerability data, event data, and flow data.

Each managed host in your deployment, including the QRadar Console, creates all backup files in the `/store/backup/` directory. Your system might include a `/store/backup` mount from an external SAN or NAS service. External services provide long term, offline retention of data, which is commonly required for compliancy regulations, such as PCI.

Restriction: You must restore the configuration backup before you restore the data backup.

Before you begin

Ensure that the following conditions are met:

- If you are restoring data on a new QRadar Console, the configuration backup is restored.
- You know the location of the managed host where the data is backed up.
- If your deployment includes a separate mount point for that volume, the `/store` or `/store/ariel` directory has sufficient space for the data that you want to recover.
- You know the date and time for the data that you want to recover.

Procedure

1. Using SSH, log in to QRadar SIEM as the root user.
2. Go to the `/store/backup` directory.
3. To list the backup files, type `ls -l`
4. If backup files are listed, go to the root directory by typing `cd /`

   Important: The restored files must be in the `/store` directory. If you type `cd` instead of `cd /`, the files are restored to the `/root/store` directory.
5. To extract the backup files to their original directory, type the following command:

   ```
   tar -zxpvPf /store/backup/backup.<name>.<hostname_hostID>
   .<target date>.<backup type>.<timestamp>.tgz
   ```

Table 42. Description of file name variables

File name variable	Description
hostname_hostID	The name of the QRadar system that hosts the backup file followed by the identifier for the QRadar system
target date	The date that the backup file was created. The format of the target date is <*day*>_<*month*>_<*year*>
backup type	The options are `data` or `config`
timestamp	The time that the backup file was created.

Results

Daily backup of data captures all data on each host. If you want to restore data on a managed host that contains only event or flow data, only that data is restored to that host.

Verifying restored data

Verify that your data is restored correctly in IBM Security QRadar.

Procedure

1. To verify that the files are restored, review the contents of one of the restored directories by typing the following command:

   ```
   cd /store/ariel/flows/payloads/<yyyy/mm/dd>
   ```

You can view the restored directories that are created for each hour of the day. If directories are missing, data might not be captured for that time period.

2. Verify that the restored data is available.
   a. Log in to the QRadar interface.
   b. Click the **Log Activity** or **Network Activity** tab.
   c. Select **Edit Search** from the **Search** list on the toolbar.
   d. In the Time Range pane of the Search window, select **Specific Interval**.
   e. Select the time range of the data you restored and then click **Filter**.
   f. View the results to verify the restored data.
   g. If your restored data is not available in the QRadar interface, verify that data is restored in the correct location and file permissions are correctly configured.

      Restored files must be in the `/store directory`. If you typed `cd` instead of `cd /` when you extracted the restored files, check the `/root/store` directory for the restored files. If you did not change directories before you extracted the restored files, check the `/store/backup/store` directory for the restored files.

      Typically, files are restored with the original permissions. However, if the files are owned by the root user account, issues might occur. If the files are owned by the root user account, change the permissions by using the **`chown`** and **`chmod`** commands.

What to do next

After you verified that your data is restored, you must reapply RPMs for any DSMs, vulnerability assessment (VA) scanners, and log source protocols.

Chapter 10. Deployment editor

Use the deployment editor to manage the individual components of your QRadar. After you configure your deployment, you can access and configure the individual components of each managed host in your deployment.

Deployment editor requirements

Before you can use the deployment editor, ensure that it meets the minimum system requirements.

The deployment editor requires Java™ Runtime Environment (JRE). You can download Java 1.6 or 1.7 from the Java website (www.java.com). If you are using the Mozilla Firefox web browser, you must configure your browser to accept Java Network Language Protocol (JNLP) files.

Many web browsers that use the Microsoft Internet Explorer engine, such as Maxthon, install components that might be incompatible with the **Admin** tab. You might be required to disable any web browsers that are installed on your system.

To access the deployment editor from behind a proxy server or firewall, you must configure the appropriate proxy settings on your desktop. The s software can then automatically detect the proxy settings from your browser.

To configure the proxy settings, open the Java configuration in your Control Pane and configure the IP address of your proxy server. For more information, see the Microsoft documentation.

Deployment editor views

The deployment editor provides the different views of your deployment.

You can access the deployment editor by using the **Admin** tab. You can use the deployment editor to create your deployment, assign connections, and configure each component.

After you update your configuration settings by using the deployment editor, you must save those changes to the staging area. You must manually deploy all changes by using the **Admin** tab menu option. All deployed changes are then enforced throughout your deployment.

The deployment editor provides the following views:

System View

Use the System View page to assign software component to managed hosts in your deployment. The System View page includes all managed hosts in your deployment. A managed host is a system in your deployment that has QRadar software that is installed.

By default, the System View page also includes the following components:

- **Host Context**, which monitors all QRadar components to ensure that each component is operating as expected.
- **Accumulator**, which analyzes flows, events, reporting, writing database data, and alerting a device system module (DSM).

  An accumulator is on any host that contains an Event Processor.

On the System View page, the left pane provides a list of managed hosts, which you can view and configure. The deployment editor polls your deployment for updates to managed hosts. If the deployment editor detects a change to a managed host in your deployment, a message is displayed notifying you of the change. For example, if you remove a managed host, a message is displayed, indicating that the assigned components to that host must be reassigned to another host.

Also, if you add a managed host to your deployment, the deployment editor displays a message that indicates that the managed host was added.

Event View

Use the Event View page to create a view of your components:

- QRadar QFlow Collector components
- Event Processors
- Event Collectors
- Off-site Sources
- Off-site Targets
- Magistrate components

On the Event View page, the left pane provides a list of components you can add to the view. The right pane provides a view of your deployment.

Vulnerability View

Use the Vulnerability View page to create a view of your IBM Security QRadar Vulnerability Manager components. You must install IBM Security QRadar Vulnerability Manager to see this view. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*

Configuring deployment editor preferences

You can configure the deployment editor preferences to modify the zoom increments and the presence poll frequency.

Procedure

1. Select **File** > **Edit Preferences**.
2. To configure the **Presence Poll Frequency**parameter, type how often, in milliseconds, you that want the managed host to monitor your deployment for updates.
3. To configure the **Zoom Increment**parameter, type the increment value when the zoom option is selected.

   For example, 0.1 indicates 10%.

Building your deployment

Use the deployment editor and options on the **Admin** tab to build and deploy your deployment.

Before you begin

Ensure that the following conditions are met:

- Install the Java Runtime Environment (JRE). You can download Java 1.6 or 1.7 from the Java website (www.java.com).
- If you are using the Firefox browser, you must configure your browser to accept Java Network Language Protocol (JNLP) files.
- Plan your QRadar deployment, including the IP addresses and login information for all devices in your deployment.

Procedure

1. Build your Event View.
2. Build your System View.
3. Configure components.
4. To stage your deployment, from the deployment editor menu, click **File** > **Save to Staging**
5. To deploy all configuration changes, on the **Admin** tab, click **Advanced** > **Deploy Changes**

Event view management

Use the Event View page to create and manage the components for your deployment.

QRadar components

QRadar deployments consist of multiple components.

QRadar deployments include the following components:

QRadar QFlow Collector

Collects data from devices, and various live and recorded feeds, such as network taps, span/mirror ports, NetFlow, and QRadar flow logs.

When the data is collected, the QRadar QFlow Collector groups related individual packets into a flow. QRadar defines these flows as a communication session between two pairs of unique IP address and ports that use the same protocol. A flow starts when the QRadar QFlow Collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options.

Each additional packet is evaluated. Counts of bytes and packets are added to the statistical counters in the flow record. At the end of an interval, a status record of the flow is sent to an Event Collector and statistical counters for the flow are reset. A flow ends when no activity for the flow is detected within the configured time.

Flow reporting generates records of all active or expired flows during a specified time. If the protocol does not support port-based connections, QRadar combines all

packets between the two hosts into a single flow record. However, a QRadar QFlow Collector does not record flows until a connection is made to another QRadar component and data is retrieved.

Event Collector

Collects security events from various types of security devices, which are known as log sources, in your network.

The Event Collector gathers events from local and remote log sources. The Event Collector then normalizes the events and sends the information to the Event Processor. The Event Collector also bundles all identical events to conserve system usage.

A non-Console Event Processor can be connected to the Event Processor on the QRadar Console or connected to another Event Processor in your deployment. The Accumulator is responsible for gathering flow and event information from the Event Processor.

The Event Processor on the QRadar Console is always connected to the Magistrate. This connection cannot be deleted.

Off-site Source

Indicates an off-site data source that forwards normalized data to an Event Collector. You can configure an off-site source to receive data and allows the data to be encrypted before forwarding.

Off-site Target

Indicates an off-site device that receives event or flow data. An off-site target can receive data only from an Event Collector.

Magistrate

The Magistrate component provides the core processing components of your system. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the events or flows against the defined custom rules to create an response. If no custom rules exist, the Magistrate uses the default rule set to process the offending event or flow.

The response is processed by using multiple inputs, individualevents or flows, and combined events or flows with analyzed behavior and vulnerabilities. Magistrate prioritizes the response and assigns a magnitude value that is based on several factors, including the amount of responses, severity, relevance, and credibility.

When processed, the Magistrate produces a list for each source, providing you with a list of attackers and their response for each event or flow. After the Magistrate establishes the magnitude, the Magistrate then provides multiple options for resolution.

By default, the Event View page includes a Magistrate component.

Process to build your Event View

To build your Event View, do the following steps:

1. Add components to your view.
2. Connect the components.
3. Connect deployments.
4. Rename the components so each component has a unique name.

Adding components

When you configure your deployment, you must use the Event View page in the deployment editor to add your components.

You can add the following QRadar components to your Event View page:

- Event Collector
- Event Processor
- Off-site source
- Off-site target
- QRadar QFlow Collector

Procedure

1. On the **Admin** tab, click **Deployment Editor**.
2. In the Event Components pane, select a component that you want to add to your deployment.
3. Type a unique name for the component you want to add and click **Next**.

   Restriction: The name can be up to 20 characters in length and might include underscores or hyphens.
4. From the **Select a host to assign to** list box, select a managed host, and then click **Next**.
5. Click **Finish**.
6. Repeat steps 3 - 5 for each component you want to add to your view.
7. From the deployment editor menu, select **File > Save to staging**.

   The deployment editor saves your changes to the staging area and automatically closes.
8. On the **Admin** tab menu, click **Deploy Changes**.

Connecting components

After you add all the necessary components in your Event View page, you must connect them.

About this task

Use the Event View page to connect components together. Some restrictions are enforced. For example, you can connect an Event Collector to an Event Processor, but not a Magistrate component.

The following table describes the components that you can connect.

Table 43. Description of supported component connections

Source connection	Target connection	Description
QRadar QFlow Collector	Event Collector	A QRadar QFlow Collector can connect only to an Event Collector. A QRadar QFlow Collector cannot be connected to an Event Collector of a 15xx appliance. The number of connections is not restricted.
Event Collector	Event Processor	An Event Collector can be connected only to one Event Processor. A ConsoleEvent Collector can be connected only to a Console Event Processor. This connection cannot be removed. A non-Console Event Collector can be connected to an Event Processor on the same system. A non-Console Event Collector can be connected to a remote Event Processor, but only if the Event Processor does not exist on the Console.
Event Collector	Off-site target	The number of connections is not restricted.
Off-site source	Event Collector	The number of connections is not restricted. An Event Collector connected to an Event-only appliance cannot receive an off-site connection from system hardware that has the **Receive Flows** feature enabled. An Event Collector connected to a QFlow-only appliance cannot receive an off-site connection from a remote system if the system has the **Receive Events** feature enabled.
Event Processor	Magistrate (MPC)	Only one Event Processor can connect to a Magistrate.

Table 43. Description of supported component connections (continued)

Source connection	Target connection	Description
Event Processor	Event Processor	A Console Event Processor cannot connect to a non-Console Event Processor. A non-Console Event Processor can be connected to another Console or non-Console Event Processor, but not both at the same time. A non-Console Event Processor is connected to a Console Event Processor when a non-Console managed host is added.

Procedure

1. In the Event View page, select the component for which you want to establish a connection.
2. Click **Actions** > **Add Connection**.

   An arrow is displayed in your map. The arrow represents a connection between two components.
3. Drag the end of the arrow to the component you want to establish a connection to.
4. Optional: Configure flow filtering on a connection between a QRadar QFlow Collector and an Event Collector.
   a. Right-click the arrow between the QRadar QFlow Collector and the Event Collector and click **Configure**
   b. In the field for the **Flow Filter** parameter, type the IP addresses or CIDR addresses for the Event Collectors you want the QRadar QFlow Collector to send flows to.
5. Click **Save**.
6. Repeat these steps for all remaining components that require connections.

Forwarding normalized events and flows

To forward normalized events and flows, configure an off-site Event Collector in your current deployment to receive events and flows from an associated off-site Event Collector in the receiving deployment.

About this task

You can add the following components to your Event View page:

- An **Off-site Source** is an off-site Event Collector from which you want to receive event and flow data.

  Restriction: The off-site source must be configured with appropriate permissions to send event and flow data to the off-site target.
- An **Off-site Target**is an off-site Event Collector to which you want to send event and flow data.

Example:

To forward normalized events and flows between two deployments (A and B), where deployment B wants to receive events and flows from deployment A:

1. Configure deployment A with an off-site target to provide the IP address of the managed host that includes Event Collector B.
2. Connect Event Collector A to the off-site target.
3. In deployment B, configure an off-site source with the IP address of the managed host that includes Event Collector A and the port that Event Collector A is monitoring.

If you want to disconnect the off-site source, you must remove the connections from both deployments. From deployment A, remove the off-site target and in deployment B, remove the off-site source.

To enable encryption between deployments, you must enable encryption on both off-site source and target. Also, you must ensure the SSH public key for the off-site source (client) is available to the target (server) to ensure appropriate access. For example, to enable encryption between the off-site source and Event Collector B, you must copy the public key in the `/root/.ssh/id_rsa.pub` directory from the off-site source to Event Collector. Add the contents of the file to `/root/.ssh/authorized_keys`directory.

The following diagram shows forwarding event and flow between deployments.

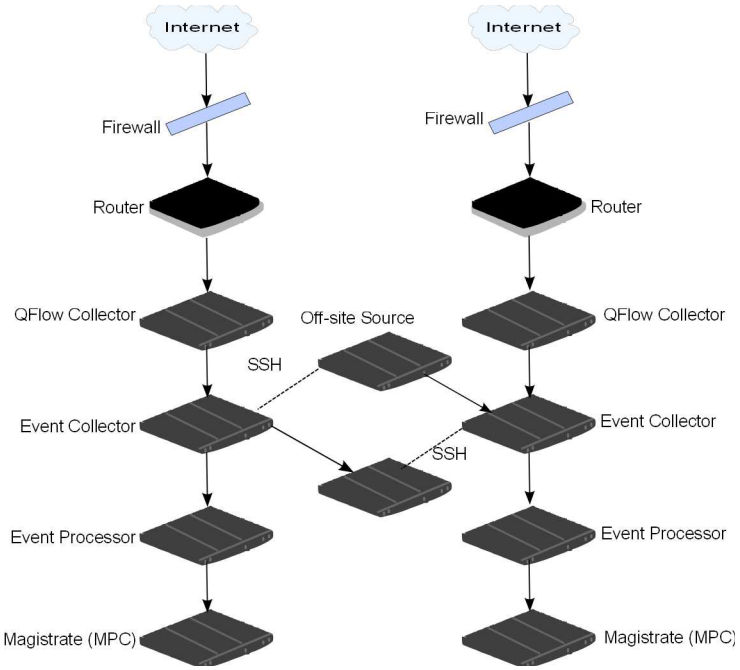

Figure 1. Forwarding events between deployments by using SSH.

If the off-site source or target is an all-in-one system, the public key is not automatically generated, therefore, you must manually generate the public key. For more information about generating public keys, see your Linux documentation.

If you update your Event Collector configuration or the monitoring ports, you must manually update your source and target configurations to maintain the connection between deployments.

Procedure

1. On the **Admin** tab, click **Deployment Editor**.
2. In the Event Components pane, select **Off-site Source** or **Off-site Target**.
3. Type a unique name for the off-site source or off-site target. The name can be up to 20 characters in length and might include underscores or hyphens. Click **Next**.
4. Enter values for the parameters and click **Finish**.

   The host name for the **Enter a name for the off-site host**field can contain a maximum of 20 characters and can include underscores or hyphens characters.

   If you select the **Encrypt traffic from off-site source** the check box, you must also select the encryption check box on the associated off-site source and target.
5. Repeat for all remaining off-site sources and targets.
6. From the deployment editor menu, click **File** > **Save to staging**.
7. On the **Admin** tab menu, select **Advanced** > **Deploy Full Configuration**.

Renaming components

You must rename a component in your view to uniquely identify components through your deployment.

Procedure

1. In the Event Components pane, select the component that you want to rename.
2. Click **Actions** > **Rename Component**.
3. Type a new name for the component.

   The name must be alphanumeric with no special characters.
4. Click **OK**.

System view management

Use the System View page to select which components you want to run on each managed host in your deployment.

Overview of the System View page

Use the System View page to manage all managed hosts in your network.

A managed host is a component in your network that includes QRadar software. If you are using a QRadar appliance, the components for that appliance model are displayed on the System View page. If your QRadar software is installed on your own hardware, the System View page includes a Host Context component.

Use the System View page to do the following tasks:

- Add managed hosts to your deployment.
- Use NAT networks in your deployment.
- Update the managed host port configuration.
- Assign a component to a managed host.
- Configure host context.
- Configure an accumulator.

Software compatibility requirements for Console and non-Console hosts

You cannot add, assign, or configure components on a non-Console managed host when the QRadar version is incompatible with the version on the Console. If a managed host was previously assigned components and is running an incompatible version, you can still view the components. However, you are not able to update or delete the components.

Encryption

Encryption provides greater security for all traffic between managed hosts. To provide enhanced security, QRadar also provides integrated support for OpenSSH. When integrated with QRadar, OpenSSH provides secure communication between components.

Encryption occurs between managed hosts in your deployment, therefore, your deployment must consist of more than one managed host before encryption is possible. Encryption is enabled by using SSH tunnels (port forwarding) initiated from the client. A client is the system that initiates a connection in a client/server relationship. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host. Encryption tunnels provide protected access to the respective servers. If you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console.

When you enable encryption on a managed host, the encryption SSH tunnel is created on the client host. For example, the connection between the Event Processor and Event Collector and the connection between the Event Processor and Magistrate are encrypted. When you enable encryption on the QRadar Console, an encryption tunnel is used when your search events by using the **Offenses** tab.

Tip: You can right-click a component to enable encryption between components.

Important: Enabling encryption reduces the performance of a managed host by at least 50%.

Adding a managed host

Use the System View page of the deployment editor to add a managed host.

Before you begin

Ensure that you installed QRadar on the managed host.

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see "NAT management" on page 130.

If you want to add a NAT-enabled managed host to a Console that is not configured to support NAT, you must disable NAT on the Console. For more information, see "Changing the NAT status for a managed host" on page 131.

Procedure

1. Click **Actions** > **Add a Managed Host**.
2. Click **Next**.

3. Enter values for the parameters.
   Use the following table to help you configure the parameters.

Table 44. Parameters for the managed host

Header	Header
Host is NATed	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
Enable Encryption	Select the check box to create an SSH encryption tunnel for the host.
	Select the check box to enable data compression between two managed hosts.

4. If you selected the **Host is NATed** check box, configure the parameters.

Table 45. Parameters for a NAT-enabled network

Parameter	Description
Enter public IP of the server or appliance to add	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
Select NATed network	If the managed host is on the same subnet as the Console, select the Console of the NAT-enabled network . If the managed host is not on the same subnet as the Console, select the managed host of the NAT-enabled network.

5. Click **Next**.
6. Click **Finish**.
7. Deploy your changes.

Related concepts:

"NAT management" on page 130
Use the deployment editor to manage NAT-enabled deployments.

Editing a managed host

Use the System View page of the deployment editor to edit a managed host.

Before you begin

If you want to enable Network Address Translation (NAT) for a managed host, the network must use static NAT translation. For more information, see "NAT management" on page 130.

If you want to add a NAT-enabled managed host to a Console that is not configured to support NAT, you must disable NAT on the Console. For more information, see "Changing the NAT status for a managed host" on page 131.

Procedure

1. Click the **System View** tab.
2. Right-click the managed host that you want to edit and select **Edit Managed Host**.

This option is available only when the selected component has a managed host that is running a compatible version of QRadar.

3. Click **Next**.
4. Edit the parameter values, as necessary.

   Use the following table to help you configure the parameters.

Table 46. Parameters for the managed host

Header	Header
Host is NATed	Select the check box to use an existing Network Address Translation (NAT) on this managed host.
Enable Encryption	Select the check box to create an SSH encryption tunnel for the host.
	Select the check box to enable data compression between two managed hosts.

5. If you selected the **Host is NATed** check box, configure the parameters.

Table 47. Parameters for a NAT-enabled network

Parameter	Description
Enter public IP of the server or appliance to add	The managed host uses this IP address to communicate with other managed hosts in different networks by using NAT.
Select NATed network	If the managed host is on the same subnet as the Console, select the Console of the NAT-enabled network . If the managed host is not on the same subnet as the Console, select the managed host of the NAT-enabled network.

6. Click **Next**.
7. Click **Finish**.

Removing a managed host

You can remove non-Console managed hosts from your deployment. You cannot remove a managed host that hosts the QRadar Console.

Tip: The **Remove host** option is available only when the selected component has a managed host that is running a compatible version of QRadar.

Procedure

1. Click the **System View** tab.
2. Right-click the managed host that you want to delete and select **Remove host**.
3. Click **OK**.
4. On the **Admin** tab menu, click**Advanced** > **Deploy Full Configuration**.

Configuring a managed host

Use the System View page of the deployment editor to configure a managed host.

Procedure

1. From the System View page, right-click the managed host that you want to configure and click **Configure**.
2. Enter values for the parameters:

   In the **Ports to exclude** field, use a comma to separate multiple ports
3. Click **Save**.

Assigning a component to a host

Use the System View page to assign the QRadar components that you added in the Event View page to the managed hosts in your deployment.

Tip: The list box displays only the managed hosts that are running a compatible version of QRadar.

Procedure

1. Click the **System View** tab.
2. From the **Managed Host** list, select the managed host that you want to assign a QRadar component to.
3. Select the component that you want to assign to a managed host.
4. From the menu, select **Actions > Assign**.
5. From the **Select a host** list box, select the host that you want to assign to this component. Click **Next**.
6. Click **Finish**.

Configuring Host Context

Use the System View page of the deployment editor to configure the Host Context component on a managed host.

The Host Context component monitors all QRadar components to make sure that each component is operating as expected.

Procedure

1. In the deployment editor, click the **System View** tab.
2. Select the managed host that includes the host context you want to configure.
3. Select the Host Context component.
4. Click **Actions** > **Configure**.
5. Enter values for the parameters.

Table 48. Host Context parameters

Parameter	Description
Warning Threshold	When the configured threshold of disk usage is exceeded, an email is sent to the administrator that indicates the current state of disk usage. The default warning threshold is 0.75. Therefore, when disk usage exceeds 75%, an email that indicates that disk usage is exceeding 75% is sent. If disk usage continues to increase above the configured threshold, a new email is sent after every 5% increase in usage. By default, Host Context monitors the following partitions for disk usage: • `/` • `/store` • `/store/tmp` **Note:** Notification emails are sent from the email address that is specified in the **Alert Email From Address** parameter to the email address specified in the **Administrative Email Address** parameter. These parameters are configured on the System Settings window. For more information, see Chapter 5, "Set up QRadar SIEM," on page 53.
Recovery Threshold	When the system exceeds the shutdown threshold, disk usage must fall below the recovery threshold before processes are restarted. The default is 0.90. Therefore, processes are not restarted until disk usage is below 90%. **Note:** Notification emails are sent from the email address that is specified in the **Alert Email From Address** parameter to the email address specified in the **Administrative Email Address** parameter. These parameters are configured on the System Settings window. For more information, see Chapter 5, "Set up QRadar SIEM," on page 53.

Table 48. Host Context parameters (continued)

Parameter	Description
Shutdown Threshold	When the system exceeds the shutdown threshold, all processes are stopped. An email is sent to the administrator that indicates the current state of the system. The default is 0.95, therefore, when disk usage exceeds 95%, all processes stop. **Note:** Notification emails are sent from the email address that is specified in the **Alert Email From Address** parameter to the email address specified in the **Administrative Email Address** parameter. These parameters are configured on the System Settings window. **Note:** For more information, see Chapter 5, "Set up QRadar SIEM," on page 53.
Inspection Interval	The frequency, in milliseconds, that you want to determine disk usage.
Inspection Interval	The frequency, in milliseconds, that you want to inspect SAR output.
Alert Interval	The frequency, in milliseconds, that you want to be notified that the threshold was exceeded.
Time Resolution	The time, in seconds, that you want the SAR inspection to be engaged.
Inspection Interval	The frequency, in milliseconds, that you want to monitor the log files.
Monitored SYSLOG File Name	A file name for the SYSLOG file.
Alert Size	The maximum number of lines you want to monitor from the log file.

6. Click **Save** .

Configuring an accumulator

Use the System View page of the deployment editor to configure the accumulator component on a managed host.

The accumulator component assists with data collection and anomaly detection for the Event Processor on a managed host. The accumulator component is responsible for receiving streams of events and flows from the local Event Processor, writing database data, and contains the anomaly detection engine (ADE).

Procedure

1. In the deployment editor, click the **System View** tab.
2. Select the managed host that you want to configure.
3. Select the accumulator component.
4. Click **Actions** > **Configure**.
5. Configure the parameters.

Table 49. Accumulator parameters

Parameter	Description
Central Accumulator	Specifies whether the current component is a central accumulator. A central accumulator exists only on a Console system.
Anomaly Detection Engine	ADE is responsible for analyzing network data and forwarding the data to the rule system for resolution. For the central accumulator, type the address and port using the following syntax: *<Console>:<port>* For a non-central accumulator, type the address and port using the following syntax: *<non-Console IP Address>:<port>*
Streamer Accumulator Listen Port	The listen port responsible for receiving streams of flows from the Event Processor. The default value is 7802.
Alerts DSM Address	The device system module (DSM) address that is used to forwarding alerts from the accumulator. Use the following syntax: *<DSM_IP address>:<DSM port number>* .

6. Click **Save**.

NAT management

Use the deployment editor to manage NAT-enabled deployments.

Network address translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and hides internal IP addresses.

You can add a non-NAT-enabled managed host by using inbound NAT for a public IP address. You can also use a dynamic IP address for outbound NAT. However, both must be on the same switch as the Console or managed host. You must configure the managed host to use the same IP address for the public and private IP addresses.

When you add or edit a managed host, you can enable NAT for that managed host. You can also use the deployment editor to manage your NAT-enabled networks.

Adding a NAT-enabled network to QRadar

Use the deployment editor to add a NAT-enabled network to your QRadar deployment.

Before you begin

Ensure that you set up your NAT-enabled networks by using static NAT translation. This setup ensures that communications between managed hosts that exist within different NAT-enabled networks.

Procedure

1. In the deployment editor, click the **NATed Networks** icon.
2. Click **Add**.
3. Type a name for a network you want to use for NAT.
4. Click **OK**.

   The Manage NATed Networks window is displayed, including the added NAT-enabled network.
5. Click **OK**.
6. Click **Yes**.

Editing a NAT-enabled network

Using the deployment editor, you can edit a NAT-enabled network.

Procedure

1. In the deployment editor, click the **NATed Networks** icon.
2. Select the NAT-enabled network that you want to edit, and click **Edit**.
3. Type a new name for of the NAT-enabled network and click **OK**.

   The Manage NATed Networks window shows the updated NAT-enabled networks.
4. Click **OK**.
5. Click **Yes**.

Deleting a NAT-enabled network from QRadar

Use the deployment editor to delete a NAT-enabled network from your deployment:

Procedure

1. In the deployment editor, click the **NATed Networks** icon.
2. Select the NAT-enabled network you want to delete.
3. Click **Delete**.
4. Click **OK**.
5. Click **Yes**.

Changing the NAT status for a managed host

Use the deployment editor to change the NAT status of a managed host in your deployment.

Before you begin

If you want to enable NAT for a managed host, the NAT-enabled network must be using static NAT translation.

To change your NAT status for a managed host, make sure you update the managed host configuration within QRadar before you update the device.

Updating the configuration first prevents the host from becoming unreachable and you can deploy changes to that host.

Procedure

1. In the deployment editor, click the **System View** tab.
2. Right-click the managed host that you want to edit and select **Edit Managed Host**.
3. Click **Next**.
4. Choose one of the following options:
   - If you want to enable NAT for the managed host, select the **Host is NATed** check box and click **Next**.
   - If you want to disable NAT for the managed host, clear the **Host is NATed** check box.

   Important: When you change the NAT status for an existing managed host, error messages might be displayed. Ignore these error messages.
5. If you enabled NAT, select a NAT-enabled network, and enter values for the parameters:

Table 50.

Parameter	Description
Change public IP of the server or appliance to add	The managed host uses this IP address to communicate with another managed host that belongs to a different network by using NAT.
Select NATed network	Update the NAT-enabled network configuration.
Manage NATs List -	Network address translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and hides internal IP addresses. For more information, see "NAT management" on page 130.

6. Click **Next**.
7. Click **Finish**.
8. Update the configuration for the device (firewall) to which the managed host is communicating.
9. On the **Admin** tab menu, click **Advanced** > **Deploy Full Configuration**.

Component configuration

Use the deployment editor to configure each component in your deployment.

Configuring a QRadar QFlow Collector

Use the deployment editor to configure a QRadar QFlow Collector.

About this task

You can configure a flow filter on the connection from a QRadar QFlow Collector and multiple Event Collectors. A flow filter controls which flow a component receives. The **Flow Filter** parameter is available on the Flow Connection Configuration window.

Right-click the arrow between the component you want to configure for flow filtering and select **Configure**.

The following table describes the advanced QRadar QFlow Collector parameters:

Procedure

1. From either the Event View or System View page, select the QRadar QFlow Collector you want to configure.
2. Click **Actions** > **Configure**.
3. Enter values for the following parameters:

Parameter	Description
Event Collector Connections	The Event Collector component that is connected to this QRadar QFlow Collector. The connection is displayed in the following format: *<Host IP Address>:<Port>*. If the QRadar QFlow Collector is not connected to an Event Collector, the parameter is empty.
QFlow CollectorID	A unique ID for the QRadar QFlow Collector.
Maximum Content Capture	The capture length, in bytes, to attach to a flow. The range is 0 - 65535. A value of 0 disables content capture. The default is 64 bytes. QRadar QFlow Collectors capture a configurable number of bytes at the start of each flow. Transferring large amounts of content across the network might affect network and performance. On managed hosts where the QRadar QFlow Collectors are on close high-speed links, you can increase the content capture length. **Important:** Increasing content capture length increases disk storage requirements for suggested disk allotment.

Parameter	Description
Alias Autodetection	The **Yes** option enables the QRadar QFlow Collector to detect external flow source aliases. When a QRadar QFlow Collector receives traffic from a device with an IP address, but no current alias, the QRadar QFlow Collector attempts a reverse DNS lookup to determine the host name of the device. If the lookup is successful, the QRadar QFlow Collector adds this information to the database and reports this information to all your deployment. The **No** option prevents the QRadar QFlow Collector from detecting external flow sources aliases.

4. On the toolbar, click **Advanced** to display the advanced parameters.
5. Enter values for the advanced parameters, as necessary.

Table 51. Advanced QRadar QFlow Collector parameters:

Parameter	Description
Event Collector Connections	The Event Collector connected to this QRadar QFlow Collector. The connection is displayed in the following format: *<Host IP Address>:<Port>*. If the QRadar QFlow Collector is not connected to an Event Collector, the parameter is empty.
Flow Routing Mode	The **0**option enables **Distributor Mode**, which allows QRadar QFlow Collectorto group flows that have similar properties. The **1** option enables **Flow Mode**, which prevents the bundling of flows
Maximum Data Capture/Packet	The number of bytes and packets that you want the QRadar QFlow Collector to capture.
Time Synchronization Server IP Address	The IP address or host name of the time server.
Time Synchronization Timeout Period	The length of time that you want the managed host to continue attempting to synchronize the time before timing out. The default is 15 minutes.
Endace DAG Interface Card Configuration	The Endace network monitoring interface card parameters. For more information about the required input for this parameter, see the IBM support website (www.ibm.com/support).

Table 51. Advanced QRadar QFlow Collector parameters: (continued)

Parameter	Description
Flow Buffer Size	The amount of memory, in MB, that you want to reserve for flow storage. The default is 400 MB.
Maximum Number of Flows	The maximum number of flows you want to send from the QRadar QFlow Collectorto an Event Collector.
Remove duplicate flows	The **Yes** option enables the QRadar QFlow Collector to remove duplicate flows. The **No**option prevents the QRadar QFlow Collector from removing duplicate flows.
Verify NetFlow Sequence Numbers	The **Yes**enables the QRadar QFlow Collector to check the incoming NetFlow sequence numbers to ensure that all packets are present and in order. A notification is displayed if a packet is missing or received out-of-order.
External Flow De-duplication method	The method that you want to use to remove duplicate external flow sources (de-duplication): • The **Source**enables the QRadar QFlow Collector to compare originating flow sources. This method compares the IP address of the device that exported the current external flow record to that of the IP address of the device that exported the first external record of the particular flow. If the IP addresses do not match, the current external flow record is discarded. • The **Record** option enables theQRadar QFlow Collector to compare individual external flow records. This method logs a list of every external flow record that is detected by a particular device and compares each subsequent record to that list. If the current record is found in the list, that record is discarded.
Flow Carry-over Window	The number of seconds before the end of an interval that you want one-sided flows to be held over until the next interval if the flow. This setting allows time for the inverse side of the flow to arrive before it is reported.

Table 51. Advanced QRadar QFlow Collector parameters: (continued)

Parameter	Description
External flow record comparison mask	• This parameter is only valid if you typed **Record** in the **External Flow De-duplication method** parameter. The external flow record fields that you want to use to remove duplicate flows include the following options: • **D** (direction) • **B** (ByteCount) • **P** (PacketCount) You can combine these options. Possible combinations of the options include the following combinations: • The **DBP** option uses direction, byte count, and packet count when it compares flow records. • The **XBP** option uses byte count and packet count when it compares flow records. • The **DXP** option uses direction and packet count when it compares flow records. • The **DBX** option uses direction and byte count when it compares flow records. • The **DXX** option uses direction when it compares flow records. • The **XBX** option uses byte count when it compares records. • The **XXP** option uses packet count when it compares records.
Create Superflows	The **Yes** option enables the QRadar QFlow Collector to create superflows from group flows that have similar properties. The **No** option prevents the creation of superflows.

Table 51. Advanced QRadar QFlow Collector parameters: (continued)

Parameter	Description
Type A Superflows	The threshold for type A superflows. A type A superflow is a group of flows from one host to many hosts. This floe is a unidirectional flow that is an aggregate of all flows that have the same different destination hosts, but following parameters are the same: • Protocol • Source bytes • Source hosts • Destination network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)
Type B Superflows	The threshold for type B superflows. A type B superflow is group of flows from many hosts to one host. This flow is unidirectional flow that is an aggregate of all flows that have different source hosts, but the following parameters are the same: • Protocol • Source bytes • Source packets • Destination host • Source network • Destination port (TCP and UDP flows only) • TCP flags (TCP flows only) • ICMP type, and code (ICMP flows only)
Type CSuperflows	The threshold for type C superflows. Type C superflows are a group of flows from one host to another host. This flow is a unidirectional flow that is an aggregate of all non-ICMP flows have different source or destination ports, but the following parameters are the same: • Protocol • Source host • Destination host • Source bytes • Destination bytes • Source packets • Destination packets

Table 51. Advanced QRadar QFlow Collector parameters: (continued)

Parameter	Description
Recombine Asymmetric Superflows	In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This routing is called asymmetric routing. You can combine flows that are received from one or more QRadar QFlow Collector. However, if you want to combine flows from multiple QRadar QFlow Collector components, you must configure flow sources in the **Asymmetric Flow Source Interface(s**) parameter in the QRadar QFlow Collector configuration. • The **Yes** option enables the QRadar QFlow Collector to recombine asymmetric flows. • The **No** option prevents the QRadar QFlow Collector from recombining asymmetric flows.
Ignore Asymmetric Superflows	The **Yes** option enables the QRadar QFlow Collector to create superflows while asymmetric flows are enabled. The **No**option prevents the QRadar QFlow Collector from creating superflows while asymmetric flows are enabled.
Minimum Buffer Data	The minimum amount of data, in bytes, that you want the Endace network monitoring interface card to receive before the captured data is returned to the QRadar QFlow Collector process. If this parameter is 0 and no data is available, the Endace network monitoring interface card allows non-blocking behavior.
Maximum Wait Time	The maximum amount of time, in microseconds, that you want the Endace network monitoring interface card to wait for the minimum amount of data. The minimum amount of data is specified in the **Minimum Buffer Data** parameter.
Polling Interval	The interval, in microseconds, that you want the Endace network monitoring interface card to wait before it checks for more data. A polling interval avoids excessive polling traffic to the card and, therefore, conserves bandwidth and processing time.

6. Click **Save**.
7. Repeat for all QRadar QFlow Collectors in your deployment you want to configure.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Configuring an Event Collector

Use the deployment editor to configure an Event Collector.

Procedure

1. From either the Event View or System View page, select the Event Collector that you want to configure.
2. Click **Actions** > **Configure**.
3. Enter values for the following parameters:

Parameter	Description
Destination Event Processor	Specifies the Event Processor component that is connected to this Event Collector. The connection is displayed in the following format: *<Host IP Address>:<Port>*.
Flow Listen Port	The listen port for flows.
Event Forwarding Listen Port	The Event Collector event forwarding port.
Flow Forwarding Listen Port	The Event Collector flow forwarding port.

4. On the toolbar, click **Advanced** to display the advanced parameters.
5. Configure the advanced parameters, as necessary.

Table 52. Event Collector advanced parameters

Parameter	Description
Primary Collector	**True**specifies that the Event Collector is on a Console system. **False** specifies that the Event Collector is on a non-Console system.
Autodetection Enabled	**Yes** enables the Event Collector to automatically analyze and accept traffic from previously unknown log sources. The appropriate firewall ports are opened to enable Autodetection to receive events. This option is the default. **No** prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources. For more information, see the *Managing Log Sources Guide*.
Flow Deduplication Filter	The amount of time in seconds that flows are buffered before they are forwarded.
Asymmetric Flow Filter	The amount of time in seconds that asymmetric flow is buffered before they are forwarded.
Forward Events Already Seen	**True** enables the Event Collector to forward events that was detected on the system. **False** prevents the Event Collector from forwarding events that was detected on the system. This option prevents event-looping on your system.

6. Click **Save**.
7. Repeat for all Event Collectors in your deployment you want to configure.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Configuring an Event Processor

Use the deployment editor to configure an Event Processor.

Procedure

1. From either the Event View or System View page, select the Event Processor that you want to configure.
2. Click **Actions** > **Configure**.
3. Enter values for the parameters:

Table 53. Parameter values for the Event Processor

Parameter	Description
Event Collector Connections Listen Port	The port that the Event Processor monitors for incoming Event Collector connections. The default value is port 32005.
Event Processor Connections Listen Port	The port that the Event Processor monitors for incoming Event Processor connections. The default value is port 32007.

4. On the toolbar, click **Advanced** to display the advanced parameters.
5. Enter values for the parameters, as necessary.

Table 54. Event Processor advanced parameters

Parameter	Description
Test Rules	The **test rules** list is available only for non-Console Event Processors. If a rule is configured to test locally, the **Globally** option does not override the rule setting. If you select**Locally**, rules are tested on the Event Processor and not shared with the system. If you select **Globally**, individual rules for every Event Processor are shared and tested system wide. Each rule can be toggled to **Global** for detection by any Event Processor on the system. For example, you can create a rule to alert you when there are five failed login attempts within 5 minutes. When the Event Processor that contains the local rule observes five failed login attempts, the rule generates a response. If the rule in the example is set to Global, when five failed login attempts within 5 minutes are detected on any Event Processor, the rule generates a response. When rules are shared globally, the rule can detect when one failed login attempt comes from five event processors. Testing rules globally is the default for non-Console Event Processor with each rule on the Event Processorset to test locally.
Overflow Event Routing Threshold	Type the events per second threshold that the Event Processor can manage. Events over this threshold are placed in the cache.
Overflow Flow Routing Threshold	Type the flows per minute threshold that the Event Processor can manage. Flows over this threshold are placed in the cache.
Events database path	Type the location that you want to store events. The default is **/store/ariel/events**.
Payloads database length	The location that you want to store payload information. The default is **/store/ariel/payloads** .

6. Click **Save**.
7. Repeat for all Event Processors in your deployment you want to configure.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Configuring the Magistrate

Use the deployment editor to configure a Magistratecomponent.

Procedure

1. From either the Event View or System View page, select the Magistrate that you want to configure.
2. Click **Actions** > **Configure**.
3. On the toolbar, click **Advanced** to display the advanced parameters.
4. In the **Overflow Routing Threshold** field, type the events per second threshold that the Magistrate can manage events.

   Events over this threshold are placed in the cache.

   The default is 20,000.
5. Click **Save**.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Configuring an off-site source

Use the deployment editor to configure an off-site source.

About this task

To prevent connection errors, when you configure off-site source and target components, deploy the QRadar Console with the off-site source first. Then deploy the QRadar Console with the off-site target.

Procedure

1. From either the Event View or System View page, select the Event Collector that you want to configure.
2. Click **Actions** > **Configure**.
3. Enter the parameter values.

Parameter	Description
Receive Events	**True** enables the system to receive events from the off-site source host. **False** prevents the system from receiving events from the off-site source host.
Receive Flows	**True** enables the system to receive flows from the off-site source host. **False** prevents the system from receiving flows from the off-site source host.

4. Click **Save**.
5. Repeat for all off-site sources in your deployment you want to configure.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Configuring an off-site target

Use the deployment editor to configure an off-site target.

About this task

To prevent connection errors, when you configure off-site source and target components, deploy the QRadar Console with the off-site source first. Then, deploy the QRadar Console with the off-site target.

Procedure

1. From either the Event View or System View page, select the Event Collector that you want to configure.
2. Click **Actions** > **Configure**.
3. Enter values for the parameters:

Parameter	Description
Event Collector Listen Port	The Event Collector listen port for receiving event data. The default port for events is 32004.
Flow Collector Listen Port	The Event Collector listening port for receiving flow data. The default port for flows is 32000.

4. Click **Save**.

Related concepts:

"QRadar components" on page 117
QRadar deployments consist of multiple components.

Chapter 11. Flow sources management

Use the Flow Sources window to manage the flow sources in your deployment.

You can add, edit, enable, disable, or delete flow sources.

Related concepts:

Chapter 11, “Flow sources management”
Use the Flow Sources window to manage the flow sources in your deployment.

Flow sources

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

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

With QRadar SIEMQRadar SIEM you can integrate flow sources.

Flow sources are classed as either internal or external:

Internal flow sources

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

- Network interface card
- Endace network monitoring interface card
- Napatech interface

External flow sources

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

External flow sources might include the following sources:

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Flowlog file

QRadar SIEM can forward external flows source data by using the spoofing or non-spoofing method:

Spoofing

Resends the inbound data that is received from flow sources to a secondary destination. To ensure that flow source data is sent to a secondary destination, configure the **Monitoring Interface** parameter in the flow source configuration to the port on which data is received (management port). When you use a specific interface, the QRadar QFlow Collector uses a promiscuous mode capture to obtain flow source data, rather than the default UDP listening port on port 2055. As a result, QRadar QFlow Collector can capture flow source packets and forward the data.

Non-Spoofing

For the non-spoofing method, configure the **Monitoring Interface** parameter in the flow source configuration as `Any`. The QRadar QFlow Collector opens the listening port, which is the port that is configured as the **Monitoring Port** to accept flow source data. The data is processed and forwarded to another flow source destination. The source IP address of the flow source data becomes the IP address of the QRadar SIEM system, not the original router that sent the data.

NetFlow

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

The process of sending data from NetFlow is often referred to as a NetFlow Data Export (NDE). You can configure IBM Security QRadar SIEM to accept NDEs and thus become a NetFlow collector. QRadar SIEM supports NetFlow versions 1, 5, 7, and 9. For more information on NetFlow, see the Cisco web site (http://www.cisco.com).

While NetFlow expands the amount of the network that is monitored, NetFlow uses a connection-less protocol (UDP) to deliver NDEs. After an NDE is sent from a switch or router, the NetFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, NetFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

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

- Make sure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the QRadar QFlow Collector configuration, you must also update your firewall access configuration.
- Make sure that the appropriate ports are configured for your QRadar QFlow Collector.

If you are using NetFlow version 9, make sure that the NetFlow template from the NetFlow source includes the following fields:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR

- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

Related concepts:

Chapter 10, “Deployment editor,” on page 115
Use the deployment editor to manage the individual components of your QRadar. After you configure your deployment, you can access and configure the individual components of each managed host in your deployment.

IPFIX

Internet Protocol Flow Information Export (IPFIX) is an accounting technology. IPFIX monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a IPFIX collector.

IBM Security Network Protection XGS 5000, a next generation intrusion protection system (IPS), is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE). IPFIX provides more flow information and deeper insight than NetFlow v9. You can configure IBM Security QRadar SIEM to accept NDEs and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After an NDE is sent from the IPFIX forwarding device, the IPFIX record might be purged.

To configure QRadar SIEM to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows by using the same process.

Your QRadar SIEM system might include a default NetFlow flow source; therefore, you might not be required to configure a NetFlow flow source. To confirm that your system includes a default NetFlow flow source, select **Admin** > **Flow Sources**. If **default_Netflow** is listed in the flow source list, IPFIX is already configured.

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

- Ensure that the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the QRadar QFlow Collector configuration, you must also update your firewall access configuration. For more information about QRadar QFlow Collector configuration, see the *IBM Security QRadar SIEM Administration Guide*.
- Ensure that the appropriate ports are configured for your QRadar QFlow Collector.
- Ensure the IPFIX template from the IPFIX source includes the following fields:
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR

- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

sFlow

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

A sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. IBM Security QRadar SIEM supports sFlow versions 2, 4, and 5. sFlow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information, see the sflow web site (www.sflow.org).

sFlow uses a connection-less protocol (UDP). When data is sent from a switch or router, the sFlow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, sFlow records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might result.

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

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

J-Flow

A proprietary accounting technology used by Juniper Networks that allows you to collect IP traffic flow statistics. J-Flow enables you to export data to a UDP port on a J-Flow collector. Using J-Flow, you can also enable J-Flow on a router or interface to collect network statistics for specific locations on your network. Note that J-Flow traffic is based on sampled data and, therefore, might not represent all network traffic. For more information on J-Flow, see the Juniper Networks website (www.juniper.net).

J-Flow uses a connection-less protocol (UDP). When data is sent from a switch or router, the J-Flow record is purged. As UDP is used to send this information and does not guarantee the delivery of data, J-Flow records inaccurate recording and reduced alerting capabilities. This can result in inaccurate presentations of both traffic volumes and bi-directional flows.

When you configure an external flow source for J-Flow, you must:

- Make sure the appropriate firewall rules are configured.
- Make sure the appropriate ports are configured for your QFlow Collector.

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 Security QRadar SIEM.

Packeteer uses a connection-less protocol (UDP). When data is sent from a switch or router, the Packeteer record is purged. As UDP is used to send this information and does not guarantee the delivery of data, Packeteer records inaccurate recording and reduced alerting capabilities. Inaccurate presentations of both traffic volumes and bidirectional flows might occur.

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

- Make sure that the appropriate firewall rules are configured.
- Make sure that you configure Packeteer devices to export flow detail records and configure the QRadar QFlow Collector as the destination for the data export.
- Make sure that the appropriate ports are configured for your QRadar QFlow Collector.
- Make sure the class IDs from the Packeteer devices can automatically be detected by the QRadar QFlow Collector.
- For more information, see the *Mapping Packeteer Applications into QRadar Technical Note*.

Flowlog file

A Flowlog file is generated from the IBM Security QRadar SIEMflow logs.

Napatech interface

If you installed a Napatech Network Adapter on your IBM Security QRadar SIEM system, the **Napatech Interface** option is displayed as a configurable packet-based flow source on the QRadar SIEM user interface. The Napatech Network Adapter provides next-generation programmable and intelligent network adapter for your network. For more information, see the Napatech documentation.

Adding or editing a flow source

Use the Flow Source window to add a flow source.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click **Flow Sources**.
5. Do one of the following actions:
   - To add a flow source, click **Add** .
   - To edit a flow source, select the flow source and click **Edit**.
6. To create this flow source from an existing flow source, select the **Build from existing flow source** check box, and select a flow source from the **Use as Template** list.
7. Enter the name for the **Flow Source Name**.

   Tip: If the external flow source is also a physical device, use the device name as the flow source name. If the flow source is not a physical device, use a recognizable name.
   For example, if you want to use IPFIX traffic, enter **ipf1**. If you want to use NetFlow traffic, enter **nf1**.

8. Select a flow source from the **Flow Source Type** list and configure the properties.
   - If you select the **Flowlog File** option, ensure that you configure the location of the Flowlog file for the **Source File Path** parameter.
   - If you select the **JFlow**, **Netflow**, **Packeteer FDR**, or **sFlow** options in the **Flow Source Type** parameter, ensure that you configure an available port for the **Monitoring Port** parameter.

     The default port for the first NetFlow flow source that is configured in your network is 2055. For each additional NetFlow flow source, the default port number increments by 1. For example, the default NetFlow flow source for the second NetFlow flow source is 2056.
   - If you select the **Napatech Interface** option, enter the **Flow Interface** that you want to assign to the flow source.

     Restriction: The **Napatech Interface** option is displayed only if you installed the Napatech Network Adapter on your system.
   - If you select the **Network Interface** option, for the **Flow Interface**, configure only one log source for each Ethernet interface.

     Restriction: You cannot send different flow types to the same port.
9. If traffic on your network is configured to take alternate paths for inbound and outbound traffic, select the **Enable Asymmetric Flows** check box.
10. Click **Save**.
11. On the **Admin** tab menu, click **Deploy Changes**.

Enabling and disabling a flow source

Using the Flow Source window, you can enable or disable a flow source.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click the **Flow Sources** icon.
5. Select the flow source that you want to enable or disable.

   The **Enabled** column indicates whether the flow source is enabled or disabled.

   The following statuses are displayed:
   - True indicates that the flow source is enabled.
   - False indicates that the flow source is now disabled.
6. Click **Enable/Disable**.
7. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a Flow Source

Use the Flow Source window to delete a flow source.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.

4. Click **Flow Sources**.
5. Select the flow source that you want to delete.
6. Click **Delete**.
7. Click **OK**.
8. On the **Admin** tab menu, click **Deploy Changes**.

Flow source aliases management

You can use the Flow Source Alias window to configure virtual names, or aliases, for your flow sources.

You can identify multiple sources that are sent to the same QRadar QFlow Collector by using the source IP address and virtual name. With an alias, a QRadar QFlow Collector can uniquely identify and process data sources that are sent to the same port.

When QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, the QRadar QFlow Collector attempts a reverse DNS lookup. The lookup is used to determine the host name of the device. If the lookup is successful, the QRadar QFlow Collector adds this information to the database and reports the information to all QRadar QFlow Collector components in your deployment.

Use the deployment editor to configure the QRadar QFlow Collector to automatically detect flow source aliases.

Adding or a flow source alias

Use the Flow Source Alias window to add a flow source alias.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click the **Flow Source Aliases** icon.
5. Do one of the following actions:
   - To add a flow source alias, click **Add** and enter the values for the parameters.
   - To edit an existing flow source alias, select the flow source alias, click **Edit**, and update the parameters.
6. Click **Save**.
7. On the **Admin** tab menu, click **Deploy Changes**.

Deleting a flow source alias

Use the Flow Source Alias window to delete a flow source alias.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. On the navigation menu, click **Flows**.
4. Click the **Flow Source Aliases** icon.

5. Select the flow source alias that you want to delete.
6. Click **Delete**.
7. Click **OK**.
8. On the **Admin** tab menu, click **Deploy Changes**.

Chapter 12. Remote networks and services configuration

Use remote network and service groups to represent traffic activity on your network for a specific profile. Remote networks groups display user traffic that originates from named remote networks.

All remote network and service groups have group levels and leaf object levels. You can edit remote network and service groups by adding objects to existing groups or changing pre-existing properties to suit your environment.

If you move an existing object to another group, the object name moves from the existing group to the newly selected group. However, when the configuration changes are deployed, the object data that is stored in the database is lost and the object ceases to function. To resolve this issue, create a new view and re-create the object that exists with another group.

On the **Admin**tab, you can group remote networks and services for use in the custom rules engine, flow, and event searches. You can also group networks and services in IBM Security QRadar Risk Manager, if it is available.

Default remote network groups

IBM Security QRadar SIEM includes default remote network groups:

The following table describes the default remote network groups.

Table 55. Default remote network groups

Group	Description
BOT	Specifies traffic that originates from BOT applications.
Bogon	Specifies traffic originating from un-assigned IP addresses. For more information, see the bogon reference on the Team CYMRU web site (http://www.team-cymru.org/Services/Bogons/).
HostileNets	Specifies traffic that originates from known hostile networks. HostileNets has a set of 20 (rank 1 - 20 inclusive) configurable CIDR ranges.
Neighbours	This group is blank by default. You must configure this group to classify traffic that originates from neighboring networks.
Smurfs	Specifies traffic that originates from smurf attacks. A smurf attack is a type of denial-of-service attack that floods a destination system with spoofed broadcast ping messages.

Table 55. Default remote network groups (continued)

Group	Description
Superflows	This group is non-configurable. A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.
TrustedNetworks	This group is blank by default. You must configure this group to classify traffic that originates from trusted networks.
Watchlists	This group is blank by default. You can configure this group to classify traffic that originates from networks you want monitor.

Groups and objects that include superflows are only for informational purposes and cannot be edited. Groups and objects that include bogons are configured by the Automatic Update function.

Default remote service groups

IBM Security QRadar SIEM includes the default remote service groups.

The following table describes the default remote service groups.

Table 56. Default remote network groups

Parameter	Description
IRC_Servers	Specifies traffic that originates from addresses commonly known as chat servers.
Online_Services	Specifies traffic that originates from addresses commonly known online services that might involve data loss.
Porn	Specifies traffic that originates from addresses commonly known to contain explicit pornographic material.
Proxies	Specifies traffic that originates from commonly known open proxy servers.
Reserved_IP_ Ranges	Specifies traffic that originates from reserved IP address ranges.
Spam	Specifies traffic that originates from addresses commonly known to produce SPAM or unwanted email.
Spy_Adware	Specifies traffic that originates from addresses commonly known to contain spyware or adware.
Superflows	Specifies traffic that originates from addresses commonly known to produce superflows.
Warez	Specifies traffic that originates from addresses commonly known to contain pirated software.

Guidelines for network resources

Given the complexities and network resources that are required for IBM Security QRadar SIEM in large structured networks, follow the suggested guidelines.

The following list describes some of the suggested practices that you can follow:

- Bundle objects and use the **Network Activity** and **Log Activity** tabs to analyze your network data.

  Fewer objects create less input and output to your disk.
- Typically, for standard system requirements, do not exceed more than 200 objects per group.

  More objects might impact your processing power when you investigate your traffic.

Managing remote networks objects

After you create remote network groups, you can aggregate flow and event search results on remote network groups. You can also create rules that test for activity on remote network groups.

Use the Remote Networks window, you can add or edit a remote networks object.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Remote Networks and Services Configuration**.
3. Click the **Remote Networks** icon.
4. To add a remote networks object, click **Add** and enter values for the parameters.
5. To edit remote networks object, click the group that you want displayed, click **Edit**, and then change the values.
6. Click **Save**.
7. Click **Return**.
8. Close the Remote Networks window.
9. On the **Admin** tab menu, click **Deploy Changes**.

Managing remote services objects

Remote services groups organize traffic that originates from user-defined network ranges or the IBM automatic update server. After you create remote service groups, you can aggregate flow and event search results, and create rules that test for activity on remote service groups.

Use the Remote Services window to add or edit a remote services object.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Remote Networks and Services Configuration**.
3. Click the **Remote Services** icon.
4. To add a remote services object, click **Add** and enter the parameter values.

5. To edit a remote services object, click the group that you want displayed, click the **Edit** icon and change the values.
6. Click **Save**.
7. Click **Return**.
8. Close the Remote Services window.
9. On the **Admin** tab menu, click **Deploy Changes**.

Chapter 13. Server discovery

The **Server Discovery** function uses the Asset Profile database to discover different server types that are based on port definitions. Then, you can select the servers to add to a server-type building block for rules.

The **Server Discovery** function is based on server-type building blocks. Ports are used to define the server type. Thus, the server-type building block works as a port-based filter when you search the Asset Profile database.

For more information about building blocks, see the *IBM Security QRadar SIEM Users Guide*.

Discovering servers

Use the **Assets** tab to discover servers on your network.

Procedure

1. Click the **Assets** tab
2. On the navigation menu, click **Server Discovery**.
3. From the **Server Type** list, select the server type that you want to discover.
4. Select one of the following options to determine the servers you want to discover:
   - To use the currently selected **Server Type** to search all servers in your deployment, select **All**.
   - To search servers in your deployment that were assigned to the currently selected **Server Type**, select **Assigned**.
   - To search servers in your deployment that are not assigned, select **Unassigned**.
5. From the **Network** list, select the network that you want to search.
6. Click **Discover Servers**.
7. In the **Matching Servers** table, select the check boxes of all servers you want to assign to the server role.
8. Click **Approve Selected Servers**.

Chapter 14. Data forwarding

You can configure IBM Security QRadar systems to forward data to one or more vendor systems, such as ticketing or alerting systems.

Forwarding Destinations

You can forward raw event and flow data that is received from log sources and flow sources to one or more vendor systems. In the user interface, these vendor systems are called forwarding destinations. You can also forward normalized data to other QRadar systems. QRadar ensures that all forwarded data is unaltered.

Configuration process for forwarding data

To configure forwarding, use the following steps:

1. Configure one or more forwarding destinations.
2. To determine what data you want to forward, configure routing rules, custom rules, or both .
3. Configure the routing options to apply to the data.

For example, you can configure all data from a specific event collector to forward to a specific ticketing system. You can also choose from various routing options such as removing the data that matches a routing rule and thereby bypassing correlation.

Adding forwarding destinations

Before you can configure bulk or selective data forwarding, you must add forwarding destinations.

Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Forwarding Destinations** icon.
4. On the toolbar, click **Add**.
5. In the Forwarding Destinations window, enter values for the parameters.

   The following table describes some of the Forwarding Destinations parameters.

Table 57. Forwarding Destinations parameters

Parameter	Description
Event Format	• **Payload** is the data in the format that the log source or flow source sent. • **Normalized** is raw data that is parsed and prepared as readable information for the user interface.
Destination Address	The IP address or host name of the vendor system that you want to forward data to.

Table 57. Forwarding Destinations parameters (continued)

Parameter	Description
Protocol	• **TCP** Use the **TCP** protocol to send normalized data by using the TCP protocol, you must create an off-site source at the destination address on port 32004. • **UDP**
Prefix a syslog header if it is missing or invalid	If a valid syslog header is not detected on the original syslog message, select this check box. The prefixed syslog header includes the QRadar SIEM appliance host IP address in the **Hostname** field of the syslog header. If this check box is not selected, the data is sent unmodified. When QRadar forwards syslog messages, the outbound message is verified to ensure that it has a valid syslog header.

6. Click **Save**.

Configuring routing rules for bulk forwarding

After you added one or more forwarding destinations, you can create filter-based routing rules to forward large quantities of data.

About this task

You can configure routing rules to forward data in either online or offline mode:

- In **Online** mode, your data remains current because forwarding is performed in real time. If the forwarding destination becomes unreachable, data can potentially be lost.
- In **Offline** mode, all data is stored in the database and then sent to the forwarding destination. This assures that no data is lost, however, there might be delays in data forwarding.

The following table describes some of the Routing Rules parameters

Table 58. Routing Rules window parameters

Parameter	Description
Forwarding Event Collector	This option is displayed when you select the **Online** option. Specifies theEvent Collector that you want this routing rule process data from.
Forwarding Event Processor	This option is displayed when you select the **Offline** option. Specifies the Event Processor that you want this routing rule process data from. **Restriction:** This option is not available if **Drop** is selected from the **Routing Options** pane.

Table 58. Routing Rules window parameters (continued)

Parameter	Description
Routing Options	• The **Forward** option specifies that data is forwarded to the specified forwarding destination. Data is also stored in the database and processed by the Custom Rules Engine (CRE). • The **Drop** option specifies that data is not stored in the database and is not processed by the CRE. The data is not forwarded to a forwarding destination, but it is processed by the CRE. This option is not available if you select the **Offline** option. • The **Bypass Correlation** option specifies that data is not processed by the CRE, but it is stored in the database. This option is not available if you select the **Offline** option. You can combine two options: • **Forward** and **Drop** Data is forwarded to the specified forwarding destination. Data is not stored in the database and is processed by the CRE. • **Forward** and **Bypass Correlation** Data is forwarded to the specified forwarding destination. Data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the data. If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database. All events are counted against the EPS license.

Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Routing Rules** icon.
4. On the toolbar, click **Add**.
5. In the Routing Rules window, enter values for the parameters.
   a. Type a name and description for your routing rule.
   b. From the **Mode** field, select one of the following options: **Online** or **Offline**.
   c. From the **Forwarding Event Collector** or **Forwarding Event Processor** list, select the event collector from which you want to forward data.

d. From the **Data Source** field in the **Event Filters** section, select which data source you want to route: **Events** or **Flows**.

   If you select the **Flow Filters** option, the section title changes to **Flow Filters** and the **Match All Incoming Events** check box changes to **Match All Flows**.

e. To forward all incoming data, select the **Match All Incoming Events** or **Match All Incoming Flows** check box.

   Restriction: If you select this check box, you cannot add a filter.

f. To add a filter, in the **Event Filters** or **Flow Filters** section, select a filter from the first list and an operand from the second list.

g. In the text box, type the value that you want to filter for, and then click **Add Filter**.

h. Repeat the previous two steps for each filter that you want to add.

i. To forward log data that matches the current filters, select the **Forward** check box, and then select the check box for each preferred forwarding destination.

   Restriction: If you select the **Forward** check box, you can also select either the **Drop** or **Bypass Correlation** check boxes, but not both of them.

   If you want to edit, add, or delete a forwarding destination, click the **Manage Destinations** link.

6. Click **Save**.

Configuring selective forwarding

Use the Custom Rule wizard to configure highly selective event data forwarding. Configure rules that forward event data to one or more forwarding destinations as a rule response.

About this task

The criteria that determines the event data that is sent to a forwarding destination is based on the tests and building blocks that are included in the rule. When the rule is configured and enabled, all event data that matches the rule tests are automatically sent to the specified forwarding destinations. For more information about how to edit or add a rule, see the see the *User Guide* for your product.

Procedure

1. Click the **OffensesLog Activity** tab.
2. On the navigation menu, select **Rules**.
3. Edit or add a rule. On the Rule Response page in the Rule wizard, ensure that you select the **Send to Forwarding Destinations** option.

Viewing forwarding destinations

The Forwarding Destinations window provides valuable information about your forwarding destinations. Statistics for the data sent to each forwarding destination is displayed.

For example, you can see the following information:

- The total number events and flows that were seen for this forwarding destination.
- The number of events or flows that were sent to this forwarding destination.

- The number of events or flows that were dropped before the forwarding destination was reached.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Forwarding Destinations** icon.
4. View the statistics for your forwarding destinations.

Viewing and managing forwarding destinations

Use the Forwarding Destination window to view, edit, and delete forwarding destinations.

Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Forwarding Destinations** icon.

   Statistics for the data sent to each forwarding destination is displayed. For example, you can see the following information:

   - The total number events and flows that were seen for this forwarding destination.
   - The number of events or flows that were sent to this forwarding destination.
   - The number of events or flows that were dropped before the forwarding destination was reached.
4. On the toolbar, click an action, as described in the following table.

Table 59. Description of the Forwarding Destination toolbar actions

Action	Description
Reset Counters	Resets the counters for the **Seen**, **Sent**, and **Dropped** parameters to zero, and the counters start accumulating again. **Tip:** You can reset the counters to provide a more targeted view of the performance of your forwarding destinations.
Edit	Changes the configured name, format, IP address, port, or protocol.
Delete	Deletes a forwarding destination If the forwarding destination is associated with any active rules, you must confirm that you want to delete the forwarding destination.

Viewing and managing routing rules

The Event Routing Rules window provides valuable information about your routing rules. You can view or manage configured filters and actions when data matches each rule.

Use the Event Routing Rules window to edit, enable, disable, or delete a rule. You can edit a routing rule to change the configured name, Event Collector, filters, or routing options.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Routing Rules** icon.
4. Select the routing rule you want to manage.
5. To edit the routing rule, on the toolbar, click **Edit** and update the parameters.
6. To remove the routing rule, on the toolbar, click **Delete**.
7. To enable or disable the routing rule, on the toolbar, click **Enable/Disable**.

   If you enable a routing rule that is configured to drop events, a confirmation message is displayed.

Chapter 15. Event store and forward

Use the Store and Forward feature to manage schedules for forwarding events from your dedicated Event Collectorappliances to Event Processorcomponents in your deployment.

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590. For more information about these appliances, see the *QRadar Hardware Guide*.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect by using the **Deployment Editor**. Use the Store and Forward feature to schedule a time range for when you want the Event Collector to forward events. During the time when events are not forwarding, the events are stored locally on the appliance. The events are not accessible in the QRadar Console user interface.

Use the scheduling feature to store events during your business hours. Forward the events to an Event Processor when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to forward events to an Event Processor during non-business hours.

Store and forward overview

The Store and Forward feature is supported on the Event Collector 1501 and Event Collector 1590 appliances. For more information on these appliances, see the *QRadar Hardware Guide* .

A dedicated Event Collector does not process events and it does not include an on-board Event Processor. By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect using the Deployment Editor. The Store and Forward feature allows you to schedule a time range for when you want the Event Collector to forward events. During the period of time when events are not forwarding, the events are stored locally on the appliance and are not accessible using the Console user interface.

This scheduling feature allows you to store events during your business hours and then forward the events to an Event Processor during periods of time when the transmission does not negatively affect your network bandwidth. For example, you can configure an Event Collector to only forward events to an Event Processor during non-business hours, such as midnight until 6 AM.

Viewing the Store and Forward schedule list

Use the Store and Forward window to see a list of schedules. The schedules include statistics that help you evaluate the status, performance, and progress of your schedules.

Before you begin

You must create a schedule. By default, the first time that you access the Store and Forward window, no schedules are listed.

About this task

You can use options on the toolbar and the **Display** list box to change your view of the schedule list. Change your view of the list to focus on the statistics from various points of view. For example, if you want to view the statistics for a particular Event Collector, you can select **Event Collectors** from the **Display** list. The list then groups by the **Event Collector** column and makes it easier for you to locate the Event Collector that you want to investigate.

By default, the Store and Forward list is configured to display the list that is organized by the schedule (**Display** > **Schedules**).

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Store and Forward** icon.
4. In the Store and Forward window, view the parameters for each schedule.

   The following table describes some of the parameters for the schedule.

Table 60. Store and Forward window parameters

Parameter	Description
Display	The **Schedules** option shows a hierarchy of the parent-child relationship between the schedules, Event Processors and the associated Event Collectors. The **Event Collectors**option shows the lowest level in the hierarchy, which is a list of Event Collectors. **Event Processors**option shows a hierarchy of the parent-child relationship between the Event Processors and the associated Event Collectors.

Table 60. Store and Forward window parameters (continued)

Parameter	Description
Name	For the **Schedules** option, the **Name** column is displayed the following format. • **First Level**represents the name of the schedule. • **Second Level**represents the name of the Event Processor. • **Third Level**represents the name of the Event Collector. For the **Event Processors**option, the column is displayed in the following format • **First Level**represents the name of the Event Processor. • **Second Level**represents the name of the Event Collector. **Tip:** You can use the plus symbol (+) and minus symbol (-) beside the name or options on the toolbar to expand and collapse the hierarchy tree. You can also expand and collapse the hierarchy tree by using options on the toolbar.
Schedule Name	Displays the name of the schedule for the **Event Collectors** or **Event Processors** options. If an Event Processor is associated with more than one schedule, the **Schedule Name** shows `Multiple`*n*, where *n* is the number of schedules. **Tip:** Click the plus symbol (+) to view the associated schedules.

Table 60. Store and Forward window parameters (continued)

Parameter	Description
Last Status	Displays the status of the Store and Forward process: • **Forwarding**indicates that event forwarding is in progress. • **Forward Complete** indicates that event forwarding is successfully completed and events are stored locally on the Event Collector. The stored events are forwarded when the schedule indicates that forwarding can start again. • **Warn** indicates that the percentage of events that are remaining in storage exceeds the percentage of time that is remaining in the Store and Forward schedule. • **Error** indicates that event forwarding was stopped before all stored events were forwarded. • **Inactive** indicates that no Event Collectors are assigned to the schedule, or the assigned Event Collectors are not receiving any events. **Tip:** Move your mouse pointer over the **Last Status** column to view a summary of the status.
Forwarded Events	Displays the number of events (in K, M, or G) forwarded in the current session. **Tip:** Move your mouse pointer over the value in the **Forwarded Events** column to view the number of events.
Remaining Events	Displays the number of events (in K, M, or G) remaining to be forwarded in the current session. **Tip:** Move your mouse pointer over the value in the **Remaining Events** column to view the number of events.
Average Event Rate	Displays the average rate at which events are forwarding from the Event Collector to the Event Processor. **Tip:** Move your mouse pointer over the value in the **Average Event Rate** column to view the average events per second (EPS).
Current Event Rate	Displays the rate at which events are forwarding from the Event Collector to the Event Processor **Tip:** Move your mouse pointer over the value in the **Current Event Rate** column to view the current events per second (EPS)

Table 60. Store and Forward window parameters (continued)

Parameter	Description
Transfer Rate Limit	The transfer rate limit is configurable. The transfer rate limit can be configured to display in kilobit per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps)..

Creating a new Store and Forward schedule

Use the Store and Forward Schedule wizard to create a schedule that controls when your Event Collector starts and stops forwarding data to an Event Processor.

You can create and manage multiple schedules to control event forwarding from multiple Event Collectors in a geographically distributed deployment.

Before you begin

Ensure that your dedicated Event Collector is added to your deployment and connected to an Event Processor. The connection between an Event Collectorand an Event Processor is configured in the **Deployment Editor**.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Store and Forward** icon.
4. Click **Actions** > **Create**.
   a. Click **Next** to move to the Select Collectors page.
   b. On the Select Collectors page, configure the parameters.

      If the Event Collector that you want to configure is not listed, it might not be added to your deployment. If so, use the **Deployment Editor** to add the Event Collector and then proceed.
   c. On the Schedule Options page, configure the parameters.

      To configure the forward transfer rate, the minimum transfer rate is 0. The maximum transfer rate is 9,999,999. A value of 0 means that the transfer rate is unlimited.
   d. Finish the configuration.

      You can now view the schedule in the Store and Forward window. After you create a new schedule, it might take up to 10 minutes for statistics to start displaying in the Store and Forward window.

Editing a Store and Forward schedule

You can edit a **Store and Forward** schedule to add or remove Event Collectors and change the schedule parameters. After you edit a **Store and Forward** schedule, the statistics that are displayed in the **Store and Forward** list are reset.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.

3. Click the **Store and Forward** icon.
4. Select the schedule that you want to edit.
5. Click **Actions** > **Edit**.

   You can also double-click a schedule for editing.
6. Click **Next** to move to the Select Collectors page.
7. On the Select Collectors page, edit the parameters.
8. Click **Next** to move to the Schedule Options page.
9. On the Schedule Options page, edit the scheduling parameters.
10. Click **Next** to move to the Summary page.
11. On the Summary page, confirm the options that you edited for this schedule.

    After you edit a schedule, it might take up to 10 minutes for statistics to update in the Store and Forward window.

Deleting a Store and Forward schedule

You can delete a **Store and Forward** schedule.

Procedure

1. On the navigation menu, click **System Configuration** .
2. Click the **Store and Forward** icon.
3. Select the schedule that you want to delete.
4. Click **Actions** > **Delete**.

   After the schedule is deleted, the associated Event Collectors resume continuous forwarding of events to their assigned Event Processor.

Chapter 16. Data obfuscation

To prevent unauthorized access to sensitive or user identifiable information, data obfuscation encrypts sensitive event data.

Any information from the event payload, such as user name, card number, or host name fields can be obfuscated. Use data obfuscation to help meet regulatory commission requirements and corporate privacy policies.

To configure and manage obfuscated data, do the following tasks:

1. Generate an RSA private/public key pair.

   The obfuscation process requires that you create a public and private key for your QRadar SIEM Console.

   Unauthorized users that attempt to query the Ariel database directly cannot view sensitive data without using the public and private decryption key.

   The public key remains on the QRadar Console and you must store the private key in a secure location. The private key contains the decryption key that is required for administrators to view the unobfuscated data.

   The `obfuscation_updater.sh` script installs the public key on your system and configures regular expression (regex) statements. The regex statements define the parameters that you want masked.
2. Configure data obfuscation.

   Data obfuscation encrypts new events as they are processed and normalized by QRadar. The obfuscation process evaluates the obfuscation expression and verifies that the raw event and normalized event contain the data that is required to mask the data. The data that is defined in the obfuscation expression is matched to the event data, encrypted, and then written to the Ariel database.

   The `obfuscation_expressions.xml` file specifies regular expression (regex) statements that identify the data that you want to obfuscate. Any text within an event that matches the regular expressions that are specified in the `obfuscation_expressions.xml` is encrypted in both the event payload and normalized fields
3. When required, decrypt data obfuscation.

   When suspicious activity occurs on your network, you can decrypt obfuscated data so that you can investigate all data that is involved in the activity.

   The `obfuscation_decoder.sh` script decrypts the specific encrypted value that you want to investigate.

Generating a private/public key pair

Data obfuscation and decryption requires an RSA private/public key pair.

Procedure

1. Using SSH, log in to your QRadar Console as the root user.
2. To generate an RSA private key, type the following command:

   `openssl genrsa [-out` *`filename`*`] [numbits]`

   The following table describes the command options.

Table 61. Command options for generating the RSA private key

Option	Description
[-out *filename*]	The file name of the RSA private key file
[numbits]	Specifies the size, in bits, of the private key The default size is 512.

Example: The following command generates a private key named mykey.pem. The size of the private key is 512 bits.

```
openssl genrsa -out mykey.pem 512
```

3. To format the private key, type the following command:

   openssl pkcs8 [-topk8] [-inform PEM] [-outform PEM] [-in *filename*] [-out *filename*] [-nocrypt]

   The following table describes the command options.

Table 62. Options to format the private key

Option	Description
[-topk8]	Reads a traditional format private key and writes the private key in PKCS #8 format
[-inform]	The input format of the private key as Privacy Enhanced Mail (.PEM) **Example:** -inform PEM
[-outform]	The format of the private key output as .PEM **Example:** -outform PEM
[-in *filename*]	The file name for the private key
[-out*filename*]	The output file name
[-nocrypt]	Specifies that the private key uses the unencrypted PrivateKeyInfo format.

Example: The following command writes the private key in PKCS #8 format and uses PEM input format. The private key is output in PEM format, is named mykey.pem, and uses an unencrypted format.

```
openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out
private_key.pem -nocrypt
```

4. To generate the RSA public key, type the following command:

   openssl rsa [-in *filename*] [-pubout] [-outform DER] [-out *filename*]

   The following table describes the command options

Table 63. Command options for generating the public key

Option	Description
[-in *filename*]	Specifies the input file name
[-pubout]	Generates a public key
[-outform DER]	The type of the public key file as DER Encoded X509 Certificate file (.DER)
[-out *filename*]	The public key file name

Example: In this example, the following keys are generated:

- mykey.pem
- private_key.pem
- public_key.der

```
openssl rsa -in mykey.pem -pubout -outform DER -out public_key.der
```

5. Delete the mykey.pem file from your system.
6. To install the public key, type the following command:

   obfuscation_updater.sh [-k *filename*]

   [-k *filename*] specifies the file name for the public key file that you want to install.

   Example: The following command installs the public key named public_key.der .

   ```
   obfuscation_updater.sh -k public_key.der
   ```

   Restriction: Only one public key can be installed for each system. After you install a public key, the key cannot be overwritten.

   After you install the public key on your QRadar Console, the QRadar Console ensures that the managed hosts obfuscate the data to match your obfuscation expression patterns.

What to do next

To avoid unauthorized access to the obfuscated data, remove the private key file from your system. Store it in a secure location and create a backup of the private key. Follow local regulations for storage of the private key.

Configuring data obfuscation

Use the obfuscation_updater.sh script to set up and configure data obfuscation.

Restriction: Events that are in the /store directory before you enable data obfuscation remain in their current state.

Any log source extensions that change the format of the event payload can cause issues with data .

Procedure

1. Using SSH, log in to your QRadar Console as the root user:
2. To configure data obfuscation, type the following command:

   You can run the obfuscation_updater.sh script from any directory on your QRadar Console.

   obfuscation_updater.sh [-p *filename*] [-e *filename*]

   [-p *filename*] specifies the private key input file name.

   [-e *filename*] specifies the obfuscation expression XML input file name.

   Example: The following command uses a file named private_key.pem as the private key and a file named obfuscation_expressions.xml as the obfuscation expression file.

   ```
   obfuscation_updater.sh -p private_key.pem -e obfuscation_expressions.xml
   ```

3. Configure the attributes of the obfuscation_expressions.xml file.

   The obfuscation_expressions.xml file defines the regular expressions that are used to obfuscate data. You can add multiple regular expressions.

   The following table describes the obfuscation_expressions.xml file attributes that you can configure.

Table 64. Attributes of the obfuscation_expressions.xml file

Attributes	Description	Database table that contains the attribute value
<expression name>	A unique name to identify the regular expression	
<regex>	The regular expression that you want to use to extract the data for obfuscation	
<captureGroup>	The capture group that is associated with the regular expression	
<deviceTypeId>	Identifies the **Log Source** type. Identifies the event and extract the data to be obfuscated.	[1]**sensordeviceType**
<deviceId>	Identifies the **Log Source**. Identifies the event and extract the data to be obfuscated.	[1]**sensordevice**
<qidId>	Identifies the **Event** name. Identifies the event and extract the data to obfuscate.	[1]**qidmap**
<category>	Identifies the low-level **Category of the Event**. Identifies the event and extract the data to be obfuscated.	[1]**Type**
<enabled>	If true, enables the regular expression. If false, disables the regular expression.	
[1]You can configure a value of -1 to disable this attribute.		

Examples of data obfuscation

1. The following code shows an example of event payload.

```
LEEF:1.0|VMware|EMC VMWare|5.1 Tue Oct 09 12:39:31 EDT
2012|jobEnable| usrName=john.smith msg=john.smith@1.1.1.1
src=1.1.1.1
```

2. The following code shows an example of an obfuscation_expressions.xml file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ObfuscationExpressions>
   <expression name="VMwareUsers">
  <regex>user (\S+)</regex>
  <deviceTypeId>-1</deviceTypeId>
  <deviceId>-1</deviceId>
```

```
  <qidId>-1</qidId>
  <category>-1</category>
  <enabled>true</enabled>
 </expression>

 <expression name="VMwarehosts">
  <regex>ruser=(\S+)</regex>
  <deviceTypeId>-1</deviceTypeId>
  <deviceId>-1</deviceId>
  <qidId>-1</qidId>
  <category>-1</category>
  <enabled>false</enabled>
 </expression>
</ObfuscationExpressions>
```

3. The following example shows the regular expressions that can parse user names.

Table 65. Example regex patterns that can parse user names.

Example regex patterns	Matches
`usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9 a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})$`	`john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com`
`usrName=(^([\w]+[^\W])([^\W]\.?)([\w]+[^\W]$))`	`john.smith, John.Smith, john, jon_smith`
`usrName=^([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\S]$\|^([a -zA-Z])[0-9_-]*[\S]$|^[a-zA-Z]*[\S]$`	`johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith`
`usrName=(/S+)`	Matches any non-white space after the equal, =, sign. This greedy regular expression can lead to system performance issues.
`msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01] ?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4 ]\d|25[0-5])\b`	Matches users with IP address. **Example:** `john.smith@1.1.1.1`
`src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01] ?\d?\d|2[0-4]\d|25[0-5])\b`	Matches IP address formats.
`host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a -zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0- 9\-]*[A-Za-z0-9])$`	`hostname.ibm.com, hostname.co.uk,`

Decrypting obfuscated data

When data obfuscation is configured on an IBM Security QRadar SIEM system, the encrypted version of the data is displayed in the columns and parameters on the user interface. Use the `obfuscation_decoder.sh` script to decrypt obfuscated data.

Procedure

1. Log in to the IBM Security QRadar SIEM user interface and copy the obfuscated text that you want to decrypt
2. Using SSH, log in to your QRadar Console as the root user.

   User name: `root`
3. Create a directory and copy the public and private keys to this directory.
4. Go to the directory where the keys are located.
5. To decrypt the obfuscated text, type the following command:

   `obfuscation_decoder.sh -k publickey` *`filename`* `-p privatekey` *`filename`* `-d` *`<obfuscated_text>`*

   The following table describes the `obfuscation_decoder.sh` options.

Table 66. Options for the `obfuscation_decoder.sh` script

Option	Description
`-k publickey` *filename*	The public key file name
`-p privatekey` *filename*	The private key file name
`-d obfuscated` *text*	The obfuscated text that you want to decrypt

Example: The following command decrypts the masked data.

```
obfuscation_decoder.sh -k public_key.der -p private_key.pem -d
obfuscated_text
```

QRadar asset profile data does not display obfuscated data after upgrade

User names and host name data that are part of the IBM Security QRadar asset profile before your upgrade to QRadar V7.2 might not display obfuscated data as expected.

Procedure

To obfuscate asset profile data, follow these steps:

1. Log in to the QRadar Console.
2. Click the **Assets** tab.
3. To remove unbofuscated hosts and user names, click **Actions** > **Delete Listed**.
4. Run scan profile manually or run schedule the scan profile to run.
5. To repopulate the data for building blocks on your QRadar system, run the **Server Discovery** tool.

Chapter 17. Audit logs

Changes that are made by QRadar users are recorded in the audit logs.

You can view the audit logs to monitor changes to QRadar and the users who change settings.

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches 200 MB. The current log file is named `audit.log`. When the file reaches 200 MB, the file is compressed and renamed to `audit.1.gz`, `audit.2.gz`. The file number increments each time that a log file is archived. QRadar stores up to 50 archived log files.

Viewing the audit log file

Use Secure Shell (SSH) to log in to your QRadar system and monitor changes to your system.

About this task

You can use **Log Activity** tab to view normalized audit log events.

The maximum size of any audit message, excluding date, time, and host name, is 1024 characters.

Each entry in the log file displays by using the following format:

```
<date_time> <host name> <user>@<IP address> (thread ID) [<category>]
[<sub-category>] [<action>] <payload>
```

The following table describes the log file format options.

Table 67. Description of the parts of the log file format

File format part	Description
date_time	The date and time of the activity in the format: Month Date HH:MM:SS
host name	The host name of the Console where this activity was logged.
user	The name of the user who changed the settings.
IP address	The IP address of the user who changed the settings.
thread ID)	The identifier of the Java thread that logged this activity.
category	The high-level category of this activity.
sub-categor	The low-level category of this activity.
action	The activity that occurred.
payload	The complete record, which might include the user record or event rule, that changed.

Procedure

1. Using SSH, log in to QRadar as the root user:
2. **User Name:** `root`
3. **Password:** *password*
4. Go to the following directory:
   `/var/log/audit`
5. Open and view the audit log file.

Logged actions

Understand the content of QRadar audit log file int the `/var/log/audit`directory. The audit log file contains logged actions.

The following list describes the categories of actions that are in the audit log file:

Administrator Authentication

- Log in to the Administration Console
- Log out of the Administration Console.

Assets

- Delete an asset.
- Delete all assets.

Audit Log Access

A search that includes events that have a high-level event category of Audit.

Backup and Recovery

- Edit the configuration.
- Initiate the backup.
- Complete the backup.
- Fail the backup.
- Delete the backup.
- Synchronize the backup.
- Cancel the backup.
- Initiate the restore.
- Upload a backup.
- Upload an invalid backup.
- Initiate the restore.
- Purge the backup.

Custom Properties

- Add a custom event property.
- Edit a custom event property.
- Delete a custom event property.
- Edit a custom flow property.
- Delete a custom flow property.

Chart Configuration

Save flow or event chart configuration.

Custom Property Expressions

- Add a custom event property expression.
- Edit a custom event property expression.
- Delete a custom event property expression.
- Add a custom flow property expression.
- Edit a custom flow property expression.
- Delete a custom flow property expression.

Retention Buckets

- Add a bucket.
- Delete a bucket.
- Edit a bucket.
- Enable or disable a bucket.

Flow Sources

- Add a flow source.
- Edit a flow source.
- Delete a flow source.

Groups

- Add a group.
- Delete a group.
- Edit a group.

High Availability

- Add a license key.
- Revert a license.
- Delete a license key.

Log Source Extension

- Add an log source extension.
- Edit the log source extension.
- Delete a log source extension.
- Upload a log source extension.
- Upload a log source extension successfully.
- Upload an invalid log source extension.
- Download a log source extension.
- Report a log source extension.
- Modify a log sources association to a device or device type.

Offenses

- Hide an offense.
- Close an offense.
- Close all offenses.
- Add a destination note.
- Add a source note.
- Add a network note.
- Add an offense note.
- Add a reason for closing offenses.
- Edit a reason for closing offenses.

Protocol Configuration

- Add a protocol configuration.
- Delete a protocol configuration.
- Edit a protocol configuration.

QIDmap

- Add a QID map entry.
- Edit a QID map entry.

QRadar Vulnerability Manager

- Create a scanner schedule.
- Update a scanner schedule.
- Delete a scanner schedule.
- Start a scanner schedule.
- Pause a scanner schedule.
- Resume a scanner schedule.

Reference Sets

- Create a reference set.
- Edit a reference set.
- Purge elements in a reference set.
- Delete a reference set.
- Add reference set elements.
- Delete reference set elements.
- Delete all reference set elements.
- Import reference set elements.
- Export reference set elements.

Reports

- Add a template.
- Delete a template.
- Edit a template.
- Generate a report.
- Delete a report.
- Delete generated content.
- View a generated report.
- Email a generated report.

Root Login

- Log in to QRadar, as root.
- Log out of QRadar, as root.

Rules

- Add a rule.
- Delete a rule.
- Edit a rule.

Scanner

- Add a scanner.
- Delete a scanner.

- Edit a scanner.

Scanner Schedule

- Add a schedule.
- Edit a schedule.
- Delete a schedule.

Session Authentication

- Create an administration session.
- Terminate an administration session.
- Deny an invalid authentication session.
- Expire a session authentication.
- Create an authentication session.
- Terminate an authentication session

SIM Clean a SIM model.

Store and Forward

- Add a Store and Forward schedule.
- Edit a Store and Forward schedule.
- Delete a Store and Forward schedule.

Syslog Forwarding

- Add a syslog forwarding.
- Delete a syslog forwarding.
- Edit a syslog forwarding.

System Management

- Shut down a system.
- Restart a system.

User Accounts

- Add an account.
- Edit an account.
- Delete an account.

User Authentication

- Log in to the user interface.
- Log out of the user interface.

User Authentication Ariel

- Deny a login attempt.
- Add an Ariel property.
- Delete an Ariel property.
- Edit an Ariel property.
- Add an Ariel property extension.
- Delete an Ariel property extension.
- Edit an Ariel property extension.

User Roles

- Add a role.
- Edit a role.
- Delete a role.

VIS

- Discover a new host.
- Discover a new operating system.
- Discover a new port.
- Discover a new vulnerability.

Chapter 18. Event categories

Event categories are used to group incoming events for processing by IBM Security QRadar. The event categories are searchable and help you monitor your network.

Events that occur on your network are aggregated into high-level and low-level categories. Each high-level category contains low-level categories and an associated severity level. You can review the severity levels that are assigned to events and adjust them to suit your corporate policy needs.

High-level event categories

Events in QRadar log sources are grouped into high-level categories. Each event is assigned to a specific high-level category.

Categorizing the incoming events ensures that you can easily search the data..

The following table describes the high-level event categories.

Table 68. High-level event categories

Category	Description
"Recon" on page 184	Events that are related to scanning and other techniques that are used to identify network resources, for example, network or host port scans.
"DoS" on page 185	Events that are related to denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.
"Authentication" on page 188	Events that are related to authentication controls, group, or privilege change, for example, log in or log out.
"Access" on page 194	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
"Exploit" on page 196	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
"Malware" on page 198	Events that are related to viruses, trojans, back door attacks, or other forms of hostile software. Malware events might include a virus, trojan, malicious software, or spyware.
"Suspicious Activity" on page 199	The nature of the threat is unknown but behavior is suspicious. The threat might include protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known intrusion detection system (IDS) evasion techniques.
"System" on page 202	Events that are related to system changes, software installation, or status messages.

Table 68. High-level event categories (continued)

Category	Description
"Policy" on page 206	Events regarding corporate policy violations or misuse.
"Unknown" on page 207	Events that are related to unknown activity on your system.
"CRE" on page 208	Events that are generated from an offense or event rule.
"Potential Exploit" on page 208	Events relate to potential application exploits and buffer overflow attempts.
"User Defined" on page 209	Events that are related to user-defined objects.
"SIM Audit" on page 212	Events that are related to user interaction with the Console and administrative functions.
"VIS Host Discovery" on page 213	Events that are related to the host, ports, or vulnerabilities that the VIS component discovers.
"Application" on page 213	Events that are related to application activity.
"Audit" on page 233	Events that are related to audit activity.
"Risk" on page 234	Events that are related to risk activity in IBM Security QRadar Risk Manager.
"Risk Manager Audit" on page 235	Events that are related to audit activity in IBM Security QRadar Risk Manager.
"Control" on page 236	Events that are related to your hardware system.
"Asset Profiler" on page 237	Events that are related to asset profiles.

Recon

The Recon category contains events that are related to scanning and other techniques that are used to identify network resources.

The following table describes the low-level event categories and associated severity levels for the Recon category.

Table 69. Low-level categories and severity levels for the Recon events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Form of Recon	An unknown form of reconnaissance.	2
Application Query	Reconnaissance to applications on your system.	3
Host Query	Reconnaissance to a host in your network.	3
Network Sweep	Reconnaissance on your network.	4
Mail Reconnaissance	Reconnaissance on your mail system.	3

Table 69. Low-level categories and severity levels for the Recon events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Windows Reconnaissance	Reconnaissance for Windows operating system.	3
Portmap / RPC r\Request	Reconnaissance on your portmap or RPC request.	3
Host Port Scan	Indicates that a scan occurred on the host ports.	4
RPC Dump	Indicates that Remote Procedure Call (RPC) information is removed.	3
DNS Reconnaissance	Reconnaissance on the DNS server.	3
Misc Reconnaissance Event	Miscellaneous reconnaissance event.	2
Web Reconnaissance	Web reconnaissance on your network.	3
Database Reconnaissance	Database reconnaissance on your network.	3
ICMP Reconnaissance	Reconnaissance on ICMP traffic.	3
UDP Reconnaissance	Reconnaissance on UDP traffic.	3
SNMP Reconnaissance	Reconnaissance on SNMP traffic.	3
ICMP Host Query	Indicates an ICMP host query.	3
UDP Host Query	Indicates a UDP host query.	3
NMAP Reconnaissance	Indicates NMAP reconnaissance.	3
TCP Reconnaissance	Indicates TCP reconnaissance on your network.	3
UNIX Reconnaissance	Reconnaissance on your UNIX network.	3
FTP Reconnaissance	Indicates FTP reconnaissance.	3

DoS

The DoS category contains events that are related to denial-of-service (DoS) attacks against services or hosts.

The following table describes the low-level event categories and associated severity levels for the DoS category.

Table 70. Low-level categories and severity levels for the DoS events category

Low-level event category	Description	Severity level (0 - 10)
Unknown DoS Attack	Indicates an unknown DoS attack.	8

Table 70. Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Description	Severity level (0 - 10)
ICMP DoS	Indicates an ICMP DoS attack.	9
TCP DoS	Indicates a TCP DoS attack.	9
UDP DoS	Indicates a UDP DoS attack.	9
DNS Service DoS	Indicates a DNS service DoS attack.	8
Web Service DoS	Indicates a web service DoS attack.	8
Mail Service DoS	Indicates a mail server DoS attack.	8
Distributed DoS	Indicates a distributed DoS attack.	9
Misc DoS	Indicates a miscellaneous DoS attack.	8
UNIX DoS	Indicates a UNIX DoS attack.	8
Windows DoS	Indicates a Windows DoS attack.	8
Database DoS	Indicates a database DoS attack.	8
FTP DoS	Indicates an FTP DoS attack.	8
Infrastructure DoS	Indicates a DoS attack on the infrastructure.	8
Telnet DoS	Indicates a Telnet DoS attack.	8
Brute Force Login	Indicates access to your system through unauthorized methods.	8
High Rate TCP DoS	Indicates a high rate TCP DoS attack.	8
High Rate UDP DoS	Indicates a high rate UDP DoS attack.	8
High Rate ICMP DoS	Indicates a high rate ICMP DoS attack.	8
High Rate DoS	Indicates a high rate DoS attack.	8
Medium Rate TCP DoS	Indicates a medium rate TCP attack.	8
Medium Rate UDP DoS	Indicates a medium rate UDP attack.	8
Medium Rate ICMP DoS	Indicates a medium rate ICMP attack.	8
Medium Rate DoS	Indicates a medium rate DoS attack.	8
Medium Rate DoS	Indicates a medium rate DoS attack.	8
Low Rate TCP DoS	Indicates a low rate TCP DoS attack.	8

Table 70. Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Low Rate UDP DoS	Indicates a low rate UDP DoS attack.	8
Low Rate ICMP DoS	Indicates a low rate ICMP DoS attack.	8
Low Rate DoS	Indicates a low rate DoS attack.	8
Distributed High Rate TCP DoS	Indicates a distributed high rate TCP DoS attack.	8
Distributed High Rate UDP DoS	Indicates a distributed high rate UDP DoS attack.	8
Distributed High Rate ICMP DoS	Indicates a distributed high rate ICMP DoS attack.	8
Distributed High Rate DoS	Indicates a distributed high rate DoS attack.	8
Distributed Medium Rate TCP DoS	Indicates a distributed medium rate TCP DoS attack.	8
Distributed Medium Rate UDP DoS	Indicates a distributed medium rate UDP DoS attack.	8
Distributed Medium Rate ICMP DoS	Indicates a distributed medium rate ICMP DoS attack.	8
Distributed Medium Rate DoS	Indicates a distributed medium rate DoS attack.	8
Distributed Low Rate TCP DoS	Indicates a distributed low rate TCP DoS attack.	8
Distributed Low Rate UDP DoS	Indicates a distributed low rate UDP DoS attack.	8
Distributed Low Rate ICMP DoS	Indicates a distributed low rate ICMP DoS attack.	8
Distributed Low Rate DoS	Indicates a distributed low rate DoS attack.	8
High Rate TCP Scan	Indicates a high rate TCP scan.	8
High Rate UDP Scan	Indicates a high rate UDP scan.	8
High Rate ICMP Scan	Indicates a high rate ICMP scan.	8
High Rate Scan	Indicates a high rate scan.	8
Medium Rate TCP Scan	Indicates a medium rate TCP scan.	8
Medium Rate UDP Scan	Indicates a medium rate UDP scan.	8
Medium Rate ICMP Scan	Indicates a medium rate ICMP scan.	8
Medium Rate Scan	Indicates a medium rate scan.	8

Table 70. Low-level categories and severity levels for the DoS events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Low Rate TCP Scan	Indicates a low rate TCP scan.	8
Low Rate UDP Scan	Indicates a low rate UDP scan.	8
Low Rate ICMP Scan	Indicates a low rate ICMP scan.	8
Low Rate Scan	Indicates a low rate scan.	8
VoIP DoS	Indicates a VoIP DoS attack.	8
Flood	Indicates a Flood attack.	8
TCP Flood	Indicates a TCP flood attack.	8
UDP Flood	Indicates a UDP flood attack.	8
ICMP Flood	Indicates an ICMP flood attack.	8
SYN Flood	Indicates a SYN flood attack.	8
URG Flood	Indicates a flood attack with the urgent (URG) flag on.	8
SYN URG Flood	Indicates a SYN flood attack with the urgent (URG) flag on.	8
SYN FIN Flood	Indicates a SYN FIN flood attack.	8
SYN ACK Flood	Indicates a SYN ACK flood attack.	8

Authentication

The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

The following table describes the low-level event categories and associated severity levels for the authentication category.

Table 71. Low-level categories and severity levels for the authentication events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Authentication	Indicates unknown authentication.	1
Host Login Succeeded	Indicates a successful host login.	1
Host Login Failed	Indicates that the host login failed.	3
Misc Login Succeeded	Indicates that the login sequence succeeded.	1
Misc Login Failed	Indicates that login sequence failed.	3
Privilege Escalation Failed	Indicates that the privileged escalation failed.	3

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Privilege Escalation Succeeded	Indicates that the privilege escalation succeeded.	1
Mail Service Login Succeeded	Indicates that the mail service login succeeded.	1
Mail Service Login Failed	Indicates that the mail service login failed.	3
Auth Server Login Failed	Indicates that the authentication server login failed.	3
Auth Server Login Succeeded	Indicates that the authentication server login succeeded.	1
Web Service Login Succeeded	Indicates that the web service login succeeded.	1
Web Service Login Failed	Indicates that the web service login failed.	3
Admin Login Successful	Indicates that an administrative login was successful.	1
Admin Login Failure	Indicates the administrative login failed.	3
Suspicious Username	Indicates that a user attempted to access the network by using an incorrect user name.	4
Login with username/ password defaults successful	Indicates that a user accessed the network by using the default user name and password.	4
Login with username/ password defaults failed	Indicates that a user was unsuccessful accessing the network by using the default user name and password.	4
FTP Login Succeeded	Indicates that the FTP login was successful.	1
FTP Login Failed	Indicates that the FTP login failed.	3
SSH Login Succeeded	Indicates that the SSH login was successful.	1
SSH Login Failed	Indicates that the SSH login failed.	2
User Right Assigned	Indicates that user access to network resources was successfully granted.	1
User Right Removed	Indicates that user access to network resources was successfully removed.	1

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Trusted Domain Added	Indicates that a trusted domain was successfully added to your deployment.	1
Trusted Domain Removed	Indicates that a trusted domain was removed from your deployment.	1
System Security Access Granted	Indicates that system security access was successfully granted.	1
System Security Access Removed	Indicates that system security access was successfully removed.	1
Policy Added	Indicates that a policy was successfully added.	1
Policy Change	Indicates that a policy was successfully changed.	1
User Account Added	Indicates that a user account was successfully added.	1
User Account Changed	Indicates a change to an existing user account.	1
Password Change Failed	Indicates that an attempt to change an existing password failed.	3
Password Change Succeeded	Indicates that a password change was successful.	1
User Account Removed	Indicates that a user account was successfully removed.	1
Group Member Added	Indicates that a group member was successfully added.	1
Group Member Removed	Indicates that a group member was removed.	1
Group Added	Indicates that a group was successfully added.	1
Group Changed	Indicates a change to an existing group.	1
Group Removed	Indicates that a group was removed.	1
Computer Account Added	Indicates that a computer account was successfully added.	1
Computer Account Changed	Indicates a change to an existing computer account.	1
Computer Account Removed	Indicates that a computer account was successfully removed.	1

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Remote Access Login Succeeded	Indicates that access to the network by using a remote login was successful.	1
Remote Access Login Failed	Indicates that an attempt to access the network byusing a remote login failed.	3
General Authentication Successful	Indicates that the authentication processes was successful.	1
General Authentication Failed	Indicates that the authentication process failed.	3
Telnet Login Succeeded	Indicates that the telnet login was successful.	1
Telnet Login Failed	Indicates that the telnet login failed.	3
Suspicious Password	Indicates that a user attempted to log in by using a suspicious password.	4
Samba Login Successful	Indicates that a user successfully logged in by using Samba.	1
Samba Login Failed	Indicates a user failed to log in by using Samba.	3
Auth Server Session Opened	Indicates that a communication session with the authentication server was started.	1
Auth Server Session Closed	Indicates that a communication session with the authentication server was closed.	1
Firewall Session Closed	Indicates that a firewall session was closed.	1
Host Logout	Indicates that a host successfully logged out.	1
Misc Logout	Indicates that a user successfully logged out.	1
Auth Server Logout	Indicates that the process to log out of the authentication server was successful.	1
Web Service Logout	Indicates that the process to log out of the web service was successful.	1
Admin Logout	Indicates that the administrative user successfully logged out.	1
FTP Logout	Indicates that the process to log out of the FTP service was successful.	1

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
SSH Logout	Indicates that the process to log out of the SSH session was successful.	1
Remote Access Logout	Indicates that the process to log out using remote access was successful.	1
Telnet Logout	Indicates that the process to log out of the Telnet session was successful.	1
Samba Logout	Indicates that the process to log out of Samba was successful.	1
SSH Session Started	Indicates that the SSH login session was initiated on a host.	1
SSH Session Finished	Indicates the termination of an SSH login session on a host.	1
Admin Session Started	Indicates that a login session was initiated on a host by an administrative or privileged user.	1
Admin Session Finished	Indicates the termination of an administrator or privileged users login session on a host.	1
VoIP Login Succeeded	Indicates a successful VoIP service login	1
VoIP Login Failed	Indicates an unsuccessful attempt to access VoIP service.	1
VoIP Logout	Indicates a user logout,	1
VoIP Session Initiated	Indicates the beginning of a VoIP session.	1
VoIP Session Terminated	Indicates the end of a VoIP session.	1
Database Login Succeeded	Indicates a successful database login.	1
Database Login Failure	Indicates a database login attempt failed.	3
IKE Authentication Failed	Indicates a failed Internet Key Exchange (IKE) authentication was detected.	3
IKE Authentication Succeeded	Indicates that a successful IKE authentication was detected.	1
IKE Session Started	Indicates that an IKE session started.	1

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
IKE Session Ended	Indicates that an IKE session ended.	1
IKE Error	Indicates an IKE error message.	1
IKE Status	Indicates IKE status message.	1
RADIUS Session Started	Indicates that a RADIUS session started.	1
RADIUS Session Ended	Indicates a RADIUS session ended.	1
RADIUS Session Denied	Indicates that a RADIUS session was denied.	1
RADIUS Session Status	Indicates a RADIUS session status message.	1
RADIUS Authentication Failed	Indicates a RADIUS authentication failure.	3
RADIUS Authentication Successful	Indicates a RADIUS authentication succeeded.	1
TACACS Session Started	Indicates a TACACS session started.	1
TACACS Session Ended	Indicates a TACACS session ended.	1
TACACS Session Denied	Indicates that a TACACS session was denied.	1
TACACS Session Status	Indicates a TACACS session status message.	1
TACACS Authentication Successful	Indicates a TACACS authentication succeeded.	1
TACACS Authentication Failed	Indicates a TACACS authentication failure.	1
Deauthenticating Host Succeeded	Indicates that the deauthentication of a host was successful.	1
Deauthenticating Host Failed	Indicates that the deauthentication of a host failed.	3
Station Authentication Succeeded	Indicates that the station authentication was successful.	1
Station Authentication Failed	Indicates that the station authentication of a host failed.	3
Station Association Succeeded	Indicates that the station association was successful.	1
Station Association Failed	Indicates that the station association failed.	3
Station Reassociation Succeeded	Indicates that the station reassociation was successful.	1

Table 71. Low-level categories and severity levels for the authentication events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Station Reassociation Failed	Indicates that the station association failed.	3
Disassociating Host Succeeded	Indicates that the disassociating a host was successful.	1
Disassociating Host Failed	Indicates that the disassociating a host failed.	3
SA Error	Indicates a Security Association (SA) error message.	5
SA Creation Failure	Indicates a Security Association (SA) creation failure.	3
SA Established	Indicates that a Security Association (SA) connection established.	1
SA Rejected	Indicates that a Security Association (SA) connection rejected.	3
Deleting SA	Indicates the deletion of a Security Association (SA).	1
Creating SA	Indicates the creation of a Security Association (SA).	1
Certificate Mismatch	Indicates a certificate mismatch.	3
Credentials Mismatch	Indicates a credentials mismatch.	3
Admin Login Attempt	Indicates an admin login attempt.	2
User Login Attempt	Indicates a user login attempt.	2
User Login Successful	Indicates a successful user login.	1
User Login Failure	Indicates a failed user login.	3
SFTP Login Succeeded	Indicates a successful SSH File Transfer Protocol (SFTP) login.	1
SFTP Login Failed	Indicates a failed SSH File Transfer Protocol (SFTP) login.	3
SFTP Logout	Indicates an SSH File Transfer Protocol (SFTP) logout.	1

Access

The access category contains authentication and access controls that are used for monitoring network events.

The following table describes the low-level event categories and associated severity levels for the access category.

Table 72. Low-level categories and severity levels for the access events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Network Communication Event	Indicates an unknown network communication event.	3
Firewall Permit	Indicates that access to the firewall was allowed.	0
Firewall Deny	Indicates that access to the firewall was denied.	4
Flow Context Response	Indicates events from the Classification Engine in response to a SIM request.	5
Misc Network Communication Event	Indicates a miscellaneous communications event.	3
IPS Deny	Indicates Intrusion Prevention Systems (IPS) denied traffic.	4
Firewall Session Opened	Indicates that the firewall session was opened.	0
Firewall Session Closed	Indicates that the firewall session was closed.	0
Dynamic Address Translation Successful	Indicates that dynamic address translation was successful.	0
No Translation Group Found	Indicates that no translation group was found.	2
Misc Authorization	Indicates that access was granted to a miscellaneous authentication server.	2
ACL Permit	Indicates that an Access Control List (ACL) allowed access.	0
ACL Deny	Indicates that an Access Control List (ACL) denied access.	4
Access Permitted	Indicates that access was allowed.	0
Access Denied	Indicates that access was denied.	4
Session Opened	Indicates that a session was opened.	1
Session Closed	Indicates that a session was closed.	1
Session Reset	Indicates that a session was reset.	3
Session Terminated	Indicates that a session was allowed.	4

Table 72. Low-level categories and severity levels for the access events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Session Denied	Indicates that a session was denied.	5
Session in Progress	Indicates that a session is in progress.	1
Session Delayed	Indicates that a session was delayed.	3
Session Queued	Indicates that a session was queued.	1
Session Inbound	Indicates that a session is inbound.	1
Session Outbound	Indicates that a session is outbound.	1
Unauthorized Access Attempt	Indicates that an unauthorized access attempt was detected.	6
Misc Application Action Allowed	Indicates that an application action was allowed.	1
Misc Application Action Denied	Indicates that an application action was denied.	3
Database Action Allowed	Indicates that a database action was allowed.	1
Database Action Denied	Indicates that a database action was denied.	3
FTP Action Allowed	Indicates that an FTP action was allowed.	1
FTP Action Denied	Indicates that an FTP action was denied.	3
Object Cached	Indicates that an object was cached.	1
Object Not Cached	Indicates that an object was not cached.	1
Rate Limiting	Indicates that the network rate-limits traffic.	4
No Rate Limiting	Indicates that the network does not rate-limit traffic.	0

Exploit

The exploit category contains events where a communication or an access exploit occurred.

The following table describes the low-level event categories and associated severity levels for the exploit category.

Table 73. Low-level categories and severity levels for the exploit events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Exploit Attack	Indicates an unknown exploit attack.	9
Buffer Overflow	Indicates a buffer overflow.	9
DNS Exploit	Indicates a DNS exploit.	9
Telnet Exploit	Indicates a Telnet exploit.	9
Linux Exploit	Indicates a Linux exploit.	9
UNIX Exploit	Indicates a UNIX exploit.	9
Windows Exploit	Indicates a Microsoft Windows exploit.	9
Mail Exploit	Indicates a mail server exploit.	9
Infrastructure Exploit	Indicates an infrastructure exploit.	9
Misc Exploit	Indicates a miscellaneous exploit.	9
Web Exploit	Indicates a web exploit.	9
Session Hijack	Indicates that a session in your network was interceded.	9
Worm Active	Indicates an active worm.	10
Password Guess/Retrieve	Indicates that a user requested access to their password information from the database.	9
FTP Exploit	Indicates an FTP exploit.	9
RPC Exploit	Indicates an RPC exploit.	9
SNMP Exploit	Indicates an SNMP exploit.	9
NOOP Exploit	Indicates an NOOP exploit.	9
Samba Exploit	Indicates a Samba exploit.	9
Database Exploit	Indicates a database exploit.	9
SSH Exploit	Indicates an SSH exploit.	9
ICMP Exploit	Indicates an ICMP exploit.	9
UDP Exploit	Indicates a UDP exploit.	9
Browser Exploit	Indicates an exploit on your browser.	9
DHCP Exploit	Indicates a DHCP exploit	9
Remote Access Exploit	Indicates a remote access exploit	9
ActiveX Exploit	Indicates an exploit through an ActiveX application.	9
SQL Injection	Indicates that an SQL injection occurred.	9
Cross-Site Scripting	Indicates a cross-site scripting vulnerability.	9

Table 73. Low-level categories and severity levels for the exploit events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Format String Vulnerability	Indicates a format string vulnerability.	9
Input Validation Exploit	Indicates that an input validation exploit attempt was detected.	9
Remote Code Execution	Indicates that a remote code execution attempt was detected.	9
Memory Corruption	Indicates that a memory corruption exploit was detected.	9
Command Execution	Indicates that a remote command execution attempt was detected.	9

Malware

The malicious software (malware) category contains events that are related to application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the malware category.

Table 74. Low-level categories and severity levels for the malware events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Malware	Indicates an unknown virus.	4
Backdoor Detected	Indicates that a back door to the system was detected.	9
Hostile Mail Attachment	Indicates a hostile mail attachment.	6
Malicious Software	Indicates a virus.	6
Hostile Software Download	Indicates a hostile software download to your network.	6
Virus Detected	Indicates that a virus was detected.	8
Misc Malware	Indicates miscellaneous malicious software	4
Trojan Detected	Indicates that a trojan was detected.	7
Spyware Detected	Indicates that spyware was detected on your system.	6
Content Scan	Indicates that an attempted scan of your content was detected.	3
Content Scan Failed	Indicates that a scan of your content failed.	8

Table 74. Low-level categories and severity levels for the malware events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Content Scan Successful	Indicates that a scan of your content was successful.	3
Content Scan in Progress	Indicates that a scan of your content is in progress.	3
Keylogger	Indicates that a key logger was detected.	7
Adware Detected	Indicates that Ad-Ware was detected.	4
Quarantine Successful	Indicates that a quarantine action successfully completed.	3
Quarantine Failed	Indicates that a quarantine action failed.	8

Suspicious Activity

The suspicious category contains events that are related to viruses, trojans, back door attacks, and other forms of hostile software.

The following table describes the low-level event categories and associated severity levels for the suspicious activity category.

Table 75. Low-level categories and severity levels for the suspicious activity events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Suspicious Event	Indicates an unknown suspicious event.	3
Suspicious Pattern Detected	Indicates that a suspicious pattern was detected.	3
Content Modified By Firewall	Indicates that content was modified by the firewall.	3
Invalid Command or Data	Indicates an invalid command or data.	3
Suspicious Packet	Indicates a suspicious packet.	3
Suspicious Activity	Indicates suspicious activity.	3
Suspicious File Name	Indicates a suspicious file name.	3
Suspicious Port Activity	Indicates suspicious port activity.	3
Suspicious Routing	Indicates suspicious routing.	3
Potential Web Vulnerability	Indicates potential web vulnerability.	3
Unknown Evasion Event	Indicates an unknown evasion event.	5
IP Spoof	Indicates an IP spoof.	5
IP Fragmentation	Indicates IP fragmentation.	3

Table 75. Low-level categories and severity levels for the suspicious activity events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Overlapping IP Fragments	Indicates overlapping IP fragments.	5
IDS Evasion	Indicates an IDS evasion.	5
DNS Protocol Anomaly	Indicates a DNS protocol anomaly.	3
FTP Protocol Anomaly	Indicates an FTP protocol anomaly.	3
Mail Protocol Anomaly	Indicates a mail protocol anomaly.	3
Routing Protocol Anomaly	Indicates a routing protocol anomaly.	3
Web Protocol Anomaly	Indicates a web protocol anomaly.	3
SQL Protocol Anomaly	Indicates an SQL protocol anomaly.	3
Executable Code Detected	Indicates that an executable code was detected.	5
Misc Suspicious Event	Indicates a miscellaneous suspicious event.	3
Information Leak	Indicates an information leak.	1
Potential Mail Vulnerability	Indicates a potential vulnerability in the mail server.	4
Potential Version Vulnerability	Indicates a potential vulnerability in the IBM Security QRadar SIEM version.	4
Potential FTP Vulnerability	Indicates a potential FTP vulnerability.	4
Potential SSH Vulnerability	Indicates a potential SSH vulnerability.	4
Potential DNS Vulnerability	Indicates a potential vulnerability in the DNS server.	4
Potential SMB Vulnerability	Indicates a potential SMB (Samba) vulnerability.	4
Potential Database Vulnerability	Indicates a potential vulnerability in the database.	4
IP Protocol Anomaly	Indicates a potential IP protocol anomaly	3
Suspicious IP Address	Indicates that a suspicious IP address was detected.	2
Invalid IP Protocol Usage	Indicates an invalid IP protocol.	2
Invalid Protocol	Indicates an invalid protocol.	4

Table 75. Low-level categories and severity levels for the suspicious activity events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Suspicious Window Events	Indicates a suspicious event with a screen on your desktop.	2
Suspicious ICMP Activity	Indicates suspicious ICMP activity.	2
Potential NFS Vulnerability	Indicates a potential network file system (NFS) vulnerability.	4
Potential NNTP Vulnerability	Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.	4
Potential RPC Vulnerability	Indicates a potential RPC vulnerability.	4
Potential Telnet Vulnerability	Indicates a potential Telnet vulnerability on your system.	4
Potential SNMP Vulnerability	Indicates a potential SNMP vulnerability.	4
Illegal TCP Flag Combination	Indicates that an invalid TCP flag combination was detected.	5
Suspicious TCP Flag Combination	Indicates that a potentially invalid TCP flag combination was detected.	4
Illegal ICMP Protocol Usage	Indicates that an invalid use of the ICMP protocol was detected.	5
Suspicious ICMP Protocol Usage	Indicates that a potentially invalid use of the ICMP protocol was detected.	4
Illegal ICMP Type	Indicates that an invalid ICMP type was detected.	5
Illegal ICMP Code	Indicates that an invalid ICMP code was detected.	5
Suspicious ICMP Type	Indicates that a potentially invalid ICMP type was detected.	4
Suspicious ICMP Code	Indicates that a potentially invalid ICMP code was detected.	4
TCP port 0	Indicates a TCP packet uses a reserved port (0) for source or destination.	4
UDP port 0	Indicates a UDP packet uses a reserved port (0) for source or destination.	4
Hostile IP	Indicates the use of a known hostile IP address.	4

Table 75. Low-level categories and severity levels for the suspicious activity events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Watch list IP	Indicates the use of an IP address from a watch list of IP addresses.	4
Known offender IP	Indicates the use of an IP address of a known offender.	4
RFC 1918 (private) IP	Indicates the use of an IP address from a private IP address range.	4
Potential VoIP Vulnerability	Indicates a potential VoIP vulnerability.	4
Blacklist Address	Indicates that an IP address is on the black list.	8
Watchlist Address	Indicates that the IP address is on the list of IP addresses being monitored.	7
Darknet Address	Indicates that the IP address is part of a darknet.	5
Botnet Address	Indicates that the address is part of a botnet.	7
Suspicious Address	Indicates that the IP address must be monitored.	5
Bad Content	Indicates that bad content was detected.	7
Invalid Cert	Indicates that an invalid certificate was detected.	7
User Activity	Indicates that user activity was detected.	7
Suspicious Protocol Usage	Indicates that suspicious protocol usage was detected.	5
Suspicious BGP Activity	Indicates that suspicious Border Gateway Protocol (BGP) usage was detected.	5
Route Poisoning	Indicates that route corruption was detected.	5
ARP Poisoning	Indicates that ARP-cache poisoning was detected.	5
Rogue Device Detected	Indicates that a rogue device was detected.	5

System

The system category contains events that are related to system changes, software installation, or status messages.

The following table describes the low-level event categories and associated severity levels for the system category.

Table 76. Low-level categories and severity levels for the system events category

Low-level event category	Description	Severity level (0 - 10)
Unknown System Event	Indicates an unknown system event.	1
System Boot	Indicates a system restart.	1
System Configuration	Indicates a change in the system configuration.	1
System Halt	Indicates that the system was halted.	1
System Failure	Indicates a system failure.	6
System Status	Indicates any information event.	1
System Error	Indicates a system error.	3
Misc System Event	Indicates a miscellaneous system event.	1
Service Started	Indicates that system services started.	1
Service Stopped	Indicates that system services stopped.	1
Service Failure	Indicates a system failure.	6
Successful Registry Modification	Indicates that a modification to the registry was successful.	1
Successful Host-Policy Modification	Indicates that a modification to the host policy was successful.	1
Successful File Modification	Indicates that a modification to a file was successful.	1
Successful Stack Modification	Indicates that a modification to the stack was successful.	1
Successful Application Modification	Indicates that a modification to the application was successful.	1
Successful Configuration Modification	Indicates that a modification to the configuration was successful.	1
Successful Service Modification	Indicates that a modification to a service was successful.	1
Failed Registry Modification	Indicates that a modification to the registry failed.	1
Failed Host-Policy Modification	Indicates that a modification to the host policy failed.	1
Failed File Modification	Indicates that a modification to a file failed.	1
Failed Stack Modification	Indicates that a modification to the stack failed.	1
Failed Application Modification	Indicates that a modification to an application failed.	1

Table 76. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Failed Configuration Modification	Indicates that a modification to the configuration failed.	1
Failed Service Modification	Indicates that a modification to the service failed.	1
Registry Addition	Indicates that a new item was added to the registry.	1
Host-Policy Created	Indicates that a new entry was added to the registry.	1
File Created	Indicates that a new was created in the system.	1
Application Installed	Indicates that a new application was installed on the system.	1
Service Installed	Indicates that a new service was installed on the system.	1
Registry Deletion	Indicates that a registry entry was deleted.	1
Host-Policy Deleted	Indicates that a host policy entry was deleted.	1
File Deleted	Indicates that a file was deleted.	1
Application Uninstalled	Indicates that an application was uninstalled.	1
Service Uninstalled	Indicates that a service was uninstalled.	1
System Informational	Indicates system information.	3
System Action Allow	Indicates that an attempted action on the system was authorized.	3
System Action Deny	Indicates that an attempted action on the system was denied.	4
Cron	Indicates a crontab message.	1
Cron Status	Indicates a crontab status message.	1
Cron Failed	Indicates a crontab failure message.	4
Cron Successful	Indicates a crontab success message.	1
Daemon	Indicates a daemon message.	1
Daemon Status	Indicates a daemon status message.	1
Daemon Failed	Indicates a daemon failure message.	4
Daemon Successful	Indicates a daemon success message.	1

Table 76. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Description	Severity level (0 - 10)
Kernel	Indicates a kernel message.	1
Kernel Status	Indicates a kernel status message.	1
Kernel Failed	Indicates a kernel failure message.	
Kernel Successful	Indicates a kernel successful message.	1
Authentication	Indicates an authentication message.	1
Information	Indicates an informational message.	2
Notice	Indicates a notice message.	3
Warning	Indicates a warning message.	5
Error	Indicates an error message.	7
Critical	Indicates a critical message.	9
Debug	Indicates a debug message.	1
Messages	Indicates a generic message.	1
Privilege Access	Indicates that privilege access was attempted.	3
Alert	Indicates an alert message.	9
Emergency	Indicates an emergency message.	9
SNMP Status	Indicates an SNMP status message.	1
FTP Status	Indicates an FTP status message.	1
NTP Status	Indicates an NTP status message.	1
Access Point Radio Failure	Indicates an access point radio failure.	3
Encryption Protocol Configuration Mismatch	Indicates an encryption protocol configuration mismatch.	3
Client Device or Authentication Server Misconfigured	Indicates that a client device or authentication server was not configured properly.	5
Hot Standby Enable Failed	Indicates a hot standby enable failure.	5
Hot Standby Disable Failed	Indicates a hot standby disable failure.	5
Hot Standby Enabled Successfully	Indicates that hot standby was enabled successfully.	1
Hot Standby Association Lost	Indicates that a hot standby association was lost.	5

Table 76. Low-level categories and severity levels for the system events category (continued)

Low-level event category	Description	Severity level (0 - 10)
MainMode Initiation Failure	Indicates MainMode initiation failure.	5
MainMode Initiation Succeeded	Indicates that the MainMode initiation was successful.	1
MainMode Status	Indicates a MainMode status message was reported.	1
QuickMode Initiation Failure	Indicates that the QuickMode initiation failed.	5
Quickmode Initiation Succeeded	Indicates that the QuickMode initiation was successful.	1
Quickmode Status	Indicates a QuickMode status message was reported.	1
Invalid License	Indicates an invalid license.	3
License Expired	Indicates an expired license.	3
New License Applied	Indicates a new license applied.	1
License Error	Indicates a license error.	5
License Status	Indicates a license status message.	1
Configuration Error	Indicates that a configuration error was detected.	5
Service Disruption	Indicates that a service disruption was detected.	5
License Exceeded	Indicates that the license capabilities were exceeded.	3
Performance Status	Indicates that the performance status was reported.	1
Performance Degradation	Indicates that the performance is being degraded.	4
Misconfiguration	Indicates that an incorrect configuration was detected.	5

Policy

The policy category contains events that are related to administration of network policy and the monitoring network resources for policy violations.

The following table describes the low-level event categories and associated severity levels for the policy category.

Table 77. Low-level categories and severity levels for the policy category

Low-level event category	Description	Severity level (0 - 10)
Unknown Policy Violation	Indicates an unknown policy violation.	2

Table 77. Low-level categories and severity levels for the policy category (continued)

Low-level event category	Description	Severity level (0 - 10)
Web Policy Violation	Indicates a web policy violation.	2
Remote Access Policy Violation	Indicates a remote access policy violation.	2
IRC/IM Policy Violation	Indicates an instant messenger policy violation.	2
P2P Policy Violation	Indicates a Peer-to-Peer (P2P) policy violation.	2
IP Access Policy Violation	Indicates an IP access policy violation.	2
Application Policy Violation	Indicates an application policy violation.	2
Database Policy Violation	Indicates a database policy violation.	2
Network Threshold Policy Violation	Indicates a network threshold policy violation.	2
Porn Policy Violation	Indicates a porn policy violation.	2
Games Policy Violation	Indicates a games policy violation.	2
Misc Policy Violation	Indicates a miscellaneous policy violation.	2
Compliance Policy Violation	Indicates a compliance policy violation.	2
Mail Policy Violation	Indicates a mail policy violation.	2
IRC Policy Violation	Indicates an IRC policy violation	2
IM Policy Violation	Indicates a policy violation that is related to instant message (IM) activities.	2
VoIP Policy Violation	Indicates a VoIP policy violation	2
Succeeded	Indicates a policy successful message.	1
Failed	Indicates a policy failure message.	4

Unknown

The Unknown category contains events that are not parsed and therefore cannot be categorized.

The following table describes the low-level event categories and associated severity levels for the Unknown category.

Table 78. Low-level categories and severity levels for the Unknown category

Low-level event category	Description	Severity level (0 - 10)
Unknown	Indicates an unknown event.	3
Unknown Snort Event	Indicates an unknown Snort event.	3
Unknown Dragon Event	Indicates an unknown Dragon event.	3
Unknown Pix Firewall Event	Indicates an unknown Cisco Private Internet Exchange (PIX) Firewall event.	3
Unknown Tipping Point Event	Indicates an unknown HP TippingPoint event.	3
Unknown Windows Auth Server Event	Indicates an unknown Windows Auth Server event.	3
Unknown Nortel Event	Indicates an unknown Nortel event.	3
Stored	Indicates an unknown stored event.	3
Behavioral	Indicates an unknown behavioral event.	3
Threshold	Indicates an unknown threshold event.	3
Anomaly	Indicates an unknown anomaly event.	3

CRE

The custom rule event (CRE) category contains events that are generated from a custom offense, flow, or event rule.

The following table describes the low-level event categories and associated severity levels for the CRE category.

Table 79. Low-level categories and severity levels for the CRE category

Low-level event category	Description	Severity level (0 - 10)
Unknown CRE Event	Indicates an unknown custom rules engine event.	5
Single Event Rule Match	Indicates a single event rule match.	5
Event Sequence Rule Match	Indicates an event sequence rule match.	5
Cross-Offense Event Sequence Rule Match	Indicates a cross-offense event sequence rule match.	5
Offense Rule Match	Indicates an offense rule match.	5

Potential Exploit

The potential exploit category contains events that are related to potential application exploits and buffer overflow attempts.

The following table describes the low-level event categories and associated severity levels for the potential exploit category.

Table 80. Low-level categories and severity levels for the potential exploit category

Low-level event category	Description	Severity level (0 - 10)
Unknown Potential Exploit Attack	Indicates that a potential exploitative attack was detected.	7
Potential Buffer Overflow	Indicates that a potential buffer overflow was detected.	7
Potential DNS Exploit	Indicates that a potentially exploitative attack through the DNS server was detected.	7
Potential Telnet Exploit	Indicates that a potentially exploitative attack through Telnet was detected.	7
Potential Linux Exploit	Indicates that a potentially exploitative attack through Linux was detected.	7
Potential UNIX Exploit	Indicates that a potentially exploitative attack through UNIX was detected.	7
Potential Windows Exploit	Indicates that a potentially exploitative attack through Windows was detected.	7
Potential Mail Exploit	Indicates that a potentially exploitative attack through mail was detected.	7
Potential Infrastructure Exploit	Indicates that a potential exploitative attack on the system infrastructure was detected.	7
Potential Misc Exploit	Indicates that a potentially exploitative attack was detected.	7
Potential Web Exploit	Indicates that a potentially exploitative attack through the web was detected.	7
Potential Botnet Connection	Indicates a potentially exploitative attack that uses botnet was detected.	6
Potential Worm Activity	Indicates a potential attack that uses worm activity was detected.	6

User Defined

The User Defined category contains events that are related to user-defined objects

The following table describes the low-level event categories and associated severity levels for the User Defined category.

Table 81. Low-level categories and severity levels for the User Defined category

Low-level event category	Description	Severity level (0 - 10)
Custom Sentry Low	Indicates a low severity custom anomaly event.	3
Custom Sentry Medium	Indicates a medium severity custom anomaly event.	5
Custom Sentry High	Indicates a high severity custom anomaly event.	7
Custom Sentry 1	Indicates a custom anomaly event with a severity level of 1.	1
Custom Sentry 2	Indicates a custom anomaly event with a severity level of 2.	2
Custom Sentry 3	Indicates a custom anomaly event with a severity level of 3.	3
Custom Sentry 4	Indicates a custom anomaly event with a severity level of 4.	4
Custom Sentry 5	Indicates a custom anomaly event with a severity level of 5.	5
Custom Sentry 6	Indicates a custom anomaly event with a severity level of 6.	6
Custom Sentry 7	Indicates a custom anomaly event with a severity level of 7.	7
Custom Sentry 8	Indicates a custom anomaly event with a severity level of 8.	8
Custom Sentry 9	Indicates a custom anomaly event with a severity level of 9.	9
Custom Policy Low	Indicates a custom policy event with a low severity level.	3
Custom Policy Medium	Indicates a custom policy event with a medium severity level.	5
Custom Policy High	Indicates a custom policy event with a high severity level.	7
Custom Policy 1	Indicates a custom policy event with a severity level of 1.	1
Custom Policy 2	Indicates a custom policy event with a severity level of 2.	2

Table 81. Low-level categories and severity levels for the User Defined category (continued)

Low-level event category	Description	Severity level (0 - 10)
Custom Policy 3	Indicates a custom policy event with a severity level of 3.	3
Custom Policy 4	Indicates a custom policy event with a severity level of 4.	4
Custom Policy 5	Indicates a custom policy event with a severity level of 5.	5
Custom Policy 6	Indicates a custom policy event with a severity level of 6.	6
Custom Policy 7	Indicates a custom policy event with a severity level of 7.	7
Custom Policy 8	Indicates a custom policy event with a severity level of 8.	8
Custom Policy 9	Indicates a custom policy event with a severity level of 9.	9
Custom User Low	Indicates a custom user event with a low severity level.	3
Custom User Medium	Indicates a custom user event with a medium severity level.	5
Custom User High	Indicates a custom user event with a high severity level.	7
Custom User 1	Indicates a custom user event with a severity level of 1.	1
Custom User 2	Indicates a custom user event with a severity level of 2.	2
Custom User 3	Indicates a custom user event with a severity level of 3.	3
Custom User 4	Indicates a custom user event with a severity level of 4.	4
Custom User 5	Indicates a custom user event with a severity level of 5.	5
Custom User 6	Indicates a custom user event with a severity level of 6.	6

Table 81. Low-level categories and severity levels for the User Defined category (continued)

Low-level event category	Description	Severity level (0 - 10)
Custom User 7	Indicates a custom user event with a severity level of 7.	7
Custom User 8	Indicates a custom user event with a severity level of 8.	8
Custom User 9	Indicates a custom user event with a severity level of 9.	9

SIM Audit

The SIM Audit category contains events that are related to user interaction with the QRadar Console and administrative features.

The following table describes the low-level event categories and associated severity levels for the SIM Audit category.

Table 82. Low-level categories and severity levels for the SIM Audit category

Low-level event category	Description	Severity level (0 - 10)
SIM User Authentication	Indicates a user login or logout on the Console.	5
SIM Configuration Change	Indicates that a user changed the SIM configuration or deployment.	3
SIM User Action	Indicates that a user initiated a process, such as starting a backup or generating a report, in the SIM module.	3
Session Created	Indicates that a user session was created.	3
Session Destroyed	Indicates that a user session was destroyed.	3
Admin Session Created	Indicates that an admin session was created.	
Admin Session Destroyed	Indicates that an admin session was destroyed.	3
Session Authentication Invalid	Indicates an invalid session authentication.	5
Session Authentication Expired	Indicates that a session authentication expired.	3
Risk Manager Configuration	Indicates that a user changed the IBM Security QRadar Risk Managerconfiguration.	3

VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities that are detected on the network, the VIS component generates events. These events are sent to the Event Collector to be correlated with other security events.

The following table describes the low-level event categories and associated severity levels for the VIS host discovery category.

Table 83. Low-level categories and severity levels for the VIS host discovery category

Low-level event category	Description	Severity level (0 - 10)
New Host Discovered	Indicates that the VIS component detected a new host.	3
New Port Discovered	Indicates that the VIS component detected a new open port.	3
New Vuln Discovered	Indicates that the VIS component detected a new vulnerability.	3
New OS Discovered	Indicates that the VIS component detected a new operating system on a host.	3
Bulk Host Discovered	Indicates that the VIS component detected many new hosts in a short period.	3

Application

The application category contains events that are related to application activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the application category.

Table 84. Low-level categories and severity levels for the application category

Low-level event category	Description	Severity level (0 - 10)
Mail Opened	Indicates that an email connection was established.	1
Mail Closed	Indicates that an email connection was closed.	1
Mail Reset	Indicates that an email connection was reset.	3
Mail Terminated	Indicates that an email connection was terminated.	4
Mail Denied	Indicates that an email connection was denied.	4
Mail in Progress	Indicates that an email connection is being attempted.	1
Mail Delayed	Indicates that an email connection was delayed.	4

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Mail Queued	Indicates that an email connection was queued.	3
Mail Redirected	Indicates that an email connection was redirected.	1
FTP Opened	Indicates that an FTP connection was opened.	1
FTP Closed	Indicates that an FTP connection was closed.	1
FTP Reset	Indicates that an FTP connection was reset.	3
FTP Terminated	Indicates that an FTP connection was terminated.	4
FTP Denied	Indicates that an FTP connection was denied.	4
FTP In Progress	Indicates that an FTP connection is in progress.	1
FTP Redirected	Indicates that an FTP connection was redirected.	3
HTTP Opened	Indicates that an HTTP connection was established.	1
HTTP Closed	Indicates that an HTTP connection was closed.	1
HTTP Reset	Indicates that an HTTP connection was reset.	3
HTTP Terminated	Indicates that an HTTP connection was terminated.	4
HTTP Denied	Indicates that an HTTP connection was denied.	4
HTTP In Progress	Indicates that an HTTP connection is in progress.	1
HTTP Delayed	Indicates that an HTTP connection was delayed.	3
HTTP Queued	Indicates that an HTTP connection was queued.	1
HTTP Redirected	Indicates that an HTTP connection was redirected.	1
HTTP Proxy	Indicates that an HTTP connection is being proxied.	1
HTTPS Opened	Indicates that an HTTPS connection was established.	1
HTTPS Closed	Indicates that an HTTPS connection was closed.	1
HTTPS Reset	Indicates that an HTTPS connection was reset.	3
HTTPS Terminated	Indicates that an HTTPS connection was terminated.	4

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
HTTPS Denied	Indicates that an HTTPS connection was denied.	4
HTTPS In Progress	Indicates that an HTTPS connection is in progress.	1
HTTPS Delayed	Indicates that an HTTPS connection was delayed.	3
HTTPS Queued	Indicates that an HTTPS connection was queued.	3
HTTPS Redirected	Indicates that an HTTPS connection was redirected.	3
HTTPS Proxy	Indicates that an HTTPS connection is proxied.	1
SSH Opened	Indicates that an SSH connection was established.	1
SSH Closed	Indicates that an SSH connection was closed.	1
SSH Reset	Indicates that an SSH connection was reset.	3
SSH Terminated	Indicates that an SSH connection was terminated.	4
SSH Denied	Indicates that an SSH session was denied.	4
SSH In Progress	Indicates that an SSH session is in progress.	1
RemoteAccess Opened	Indicates that a remote access connection was established.	1
RemoteAccess Closed	Indicates that a remote access connection was closed.	1
RemoteAccess Reset	Indicates that a remote access connection was reset.	3
RemoteAccess Terminated	Indicates that a remote access connection was terminated.	4
RemoteAccess Denied	Indicates that a remote access connection was denied.	4
RemoteAccess In Progress	Indicates that a remote access connection is in progress.	1
RemoteAccess Delayed	Indicates that a remote access connection was delayed.	3
RemoteAccess Redirected	Indicates that a remote access connection was redirected.	3
VPN Opened	Indicates that a VPN connection was opened.	1
VPN Closed	Indicates that a VPN connection was closed.	1
VPN Reset	Indicates that a VPN connection was reset.	3

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
VPN Terminated	Indicates that a VPN connection was terminated.	4
VPN Denied	Indicates that a VPN connection was denied.	4
VPN In Progress	Indicates that a VPN connection is in progress.	1
VPN Delayed	Indicates that a VPN connection was delayed	3
VPN Queued	Indicates that a VPN connection was queued.	3
VPN Redirected	Indicates that a VPN connection was redirected.	3
RDP Opened	Indicates that an RDP connection was established.	1
RDP Closed	Indicates that an RDP connection was closed.	1
RDP Reset	Indicates that an RDP connection was reset.	3
RDP Terminated	Indicates that an RDP connection was terminated.	4
RDP Denied	Indicates that an RDP connection was denied.	4
RDP In Progress	Indicates that an RDP connection is in progress.	1
RDP Redirected	Indicates that an RDP connection was redirected.	3
FileTransfer Opened	Indicates that a file transfer connection was established.	1
FileTransfer Closed	Indicates that a file transfer connection was closed.	1
FileTransfer Reset	Indicates that a file transfer connection was reset.	3
FileTransfer Terminated	Indicates that a file transfer connection was terminated.	4
FileTransfer Denied	Indicates that a file transfer connection was denied.	4
FileTransfer In Progress	Indicates that a file transfer connection is in progress.	1
FileTransfer Delayed	Indicates that a file transfer connection was delayed.	3
FileTransfer Queued	Indicates that a file transfer connection was queued.	3
FileTransfer Redirected	Indicates that a file transfer connection was redirected.	3
DNS Opened	Indicates that a DNS connection was established.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
DNS Closed	Indicates that a DNS connection was closed.	1
DNS Reset	Indicates that a DNS connection was reset.	5
DNS Terminated	Indicates that a DNS connection was terminated.	5
DNS Denied	Indicates that a DNS connection was denied.	5
DNS In Progress	Indicates that a DNS connection is in progress.	1
DNS Delayed	Indicates that a DNS connection was delayed.	5
DNS Redirected	Indicates that a DNS connection was redirected.	4
Chat Opened	Indicates that a chat connection was opened.	1
Chat Closed	Indicates that a chat connection was closed.	1
Chat Reset	Indicates that a chat connection was reset.	3
Chat Terminated	Indicates that a chat connection was terminated.	3
Chat Denied	Indicates that a chat connection was denied.	3
Chat In Progress	Indicates that a chat connection is in progress.	1
Chat Redirected	Indicates that a chat connection was redirected.	1
Database Opened	Indicates that a database connection was established.	1
Database Closed	Indicates that a database connection was closed.	1
Database Reset	Indicates that a database connection was reset.	5
Database Terminated	Indicates that a database connection was terminated.	5
Database Denied	Indicates that a database connection was denied.	5
Database In Progress	Indicates that a database connection is in progress.	1
Database Redirected	Indicates that a database connection was redirected.	3
SMTP Opened	Indicates that an SMTP connection was established.	1
SMTP Closed	Indicates that an SMTP connection was closed.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
SMTP Reset	Indicates that an SMTP connection was reset.	3
SMTP Terminated	Indicates that an SMTP connection was terminated.	5
SMTP Denied	Indicates that an SMTP connection was denied.	5
SMTP In Progress	Indicates that an SMTP connection is in progress.	1
SMTP Delayed	Indicates that an SMTP connection was delayed.	3
SMTP Queued	Indicates that an SMTP connection was queued.	3
SMTP Redirected	Indicates that an SMTP connection was redirected.	3
Auth Opened	Indicates that an authorization server connection was established.	1
Auth Closed	Indicates that an authorization server connection was closed.	1
Auth Reset	Indicates that an authorization server connection was reset.	3
Auth Terminated	Indicates that an authorization server connection was terminated.	4
Auth Denied	Indicates that an authorization server connection was denied.	4
Auth In Progress	Indicates that an authorization server connection is in progress.	1
Auth Delayed	Indicates that an authorization server connection was delayed.	3
Auth Queued	Indicates that an authorization server connection was queued.	3
Auth Redirected	Indicates that an authorization server connection was redirected.	2
P2P Opened	Indicates that a Peer-to-Peer (P2P) connection was established.	1
P2P Closed	Indicates that a P2P connection was closed.	1
P2P Reset	Indicates that a P2P connection was reset.	4

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
P2P Terminated	Indicates that a P2P connection was terminated.	4
P2P Denied	Indicates that a P2P connection was denied.	3
P2P In Progress	Indicates that a P2P connection is in progress.	1
Web Opened	Indicates that a web connection was established.	1
Web Closed	Indicates that a web connection was closed.	1
Web Reset	Indicates that a web connection was reset.	4
Web Terminated	Indicates that a web connection was terminated.	4
Web Denied	Indicates that a web connection was denied.	4
Web In Progress	Indicates that a web connection is in progress.	1
Web Delayed	Indicates that a web connection was delayed.	3
Web Queued	Indicates that a web connection was queued.	1
Web Redirected	Indicates that a web connection was redirected.	1
Web Proxy	Indicates that a web connection was proxied.	1
VoIP Opened	Indicates that a Voice Over IP (VoIP) connection was established.	1
VoIP Closed	Indicates that a VoIP connection was closed.	1
VoIP Reset	Indicates that a VoIP connection was reset.	3
VoIP Terminated	Indicates that a VoIP connection was terminated.	3
VoIP Denied	Indicates that a VoIP connection was denied.	3
VoIP In Progress	Indicates that a VoIP connection is in progress.	1
VoIP Delayed	Indicates that a VoIP connection was delayed.	3
VoIP Redirected	Indicates that a VoIP connection was redirected.	3
LDAP Session Started	Indicates an LDAP session started.	1
LDAP Session Ended	Indicates an LDAP session ended.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
LDAP Session Denied	Indicates that an LDAP session was denied.	3
LDAP Session Status	Indicates that an LDAP session status message was reported.	1
LDAP Authentication Failed	Indicates that an LDAP authentication failed.	4
LDAP Authentication Succeeded	Indicates that an LDAP authentication was successful.	1
AAA Session Started	Indicates that an Authentication, Authorization, and Accounting (AAA) session started.	1
AAA Session Ended	Indicates that an AAA session ended.	1
AAA Session Denied	Indicates that an AAA session was denied.	3
AAA Session Status	Indicates that an AAA session status message was reported.	1
AAA Authentication Failed	Indicates that an AAA authentication failed.	4
AAA Authentication Succeeded	Indicates that an AAA authentication was successful.	1
IPSEC Authentication Failed	Indicates that an Internet Protocol Security (IPSEC) authentication failed.	4
IPSEC Authentication Succeeded	Indicates that an IPSEC authentication was successful.	1
IPSEC Session Started	Indicates that an IPSEC session started.	1
IPSEC Session Ended	Indicates that an IPSEC session ended.	1
IPSEC Error	Indicates that an IPSEC error message was reported.	5
IPSEC Status	Indicates that an IPSEC session status message was reported.	1
IM Session Opened	Indicates that an Instant Messenger (IM) session was established.	1
IM Session Closed	Indicates that an IM session was closed.	1
IM Session Reset	Indicates that an IM session was reset.	3

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
IM Session Terminated	Indicates that an IM session was terminated.	3
IM Session Denied	Indicates that an IM session was denied.	3
IM Session In Progress	Indicates that an IM session is in progress.	1
IM Session Delayed	Indicates that an IM session was delayed	3
IM Session Redirected	Indicates that an IM session was redirected.	3
WHOIS Session Opened	Indicates that a WHOIS session was established.	1
WHOIS Session Closed	Indicates that a WHOIS session was closed.	1
WHOIS Session Reset	Indicates that a WHOIS session was reset.	3
WHOIS Session Terminated	Indicates that a WHOIS session was terminated.	3
WHOIS Session Denied	Indicates that a WHOIS session was denied.	3
WHOIS Session In Progress	Indicates that a WHOIS session is in progress.	1
WHOIS Session Redirected	Indicates that a WHOIS session was redirected.	3
Traceroute Session Opened	Indicates that a Traceroute session was established.	1
Traceroute Session Closed	Indicates that a Traceroute session was closed.	1
Traceroute Session Denied	Indicates that a Traceroute session was denied.	3
Traceroute Session In Progress	Indicates that a Traceroute session is in progress.	1
TN3270 Session Opened	TN3270 is a terminal emulation program, which is used to connect to an IBM 3270 terminal. This category indicates that a TN3270 session was established.	1
TN3270 Session Closed	Indicates that a TN3270 session was closed.	1
TN3270 Session Reset	Indicates that a TN3270 session was reset.	3
TN3270 Session Terminated	Indicates that a TN3270 session was terminated.	3
TN3270 Session Denied	Indicates that a TN3270 session was denied.	3
TN3270 Session In Progress	Indicates that a TN3270 session is in progress.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
TFTP Session Opened	Indicates that a TFTP session was established.	1
TFTP Session Closed	Indicates that a TFTP session was closed.	1
TFTP Session Reset	Indicates that a TFTP session was reset.	3
TFTP Session Terminated	Indicates that a TFTP session was terminated.	3
TFTP Session Denied	Indicates that a TFTP session was denied.	3
TFTP Session In Progress	Indicates that a TFTP session is in progress.	1
Telnet Session Opened	Indicates that a Telnet session was established.	1
Telnet Session Closed	Indicates that a Telnet session was closed.	1
Telnet Session Reset	Indicates that a Telnet session was reset.	3
Telnet Session Terminated	Indicates that a Telnet session was terminated.	3
Telnet Session Denied	Indicates that a Telnet session was denied.	3
Telnet Session In Progress	Indicates that a Telnet session is in progress.	1
Syslog Session Opened	Indicates that a syslog session was established.	1
Syslog Session Closed	Indicates that a syslog session was closed.	1
Syslog Session Denied	Indicates that a syslog session was denied.	3
Syslog Session In Progress	Indicates that a syslog session is in progress.	1
SSL Session Opened	Indicates that a Secure Socket Layer (SSL) session was established.	1
SSL Session Closed	Indicates that an SSL session was closed.	1
SSL Session Reset	Indicates that an SSL session was reset.	3
SSL Session Terminated	Indicates that an SSL session was terminated.	3
SSL Session Denied	Indicates that an SSL session was denied.	3
SSL Session In Progress	Indicates that an SSL session is in progress.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
SNMP Session Opened	Indicates that a Simple Network Management Protocol (SNMP) session was established.	1
SNMP Session Closed	Indicates that an SNMP session was closed.	1
SNMP Session Denied	Indicates that an SNMP session was denied.	3
SNMP Session In Progress	Indicates that an SNMP session is in progress.	1
SMB Session Opened	Indicates that a Server Message Block (SMB) session was established.	1
SMB Session Closed	Indicates that an SMB session was closed.	1
SMB Session Reset	Indicates that an SMB session was reset.	3
SMB Session Terminated	Indicates that an SMB session was terminated.	3
SMB Session Denied	Indicates that an SMB session was denied.	3
SMB Session In Progress	Indicates that an SMB session is in progress.	1
Streaming Media Session Opened	Indicates that a Streaming Media session was established.	1
Streaming Media Session Closed	Indicates that a Streaming Media session was closed.	1
Streaming Media Session Reset	Indicates that a Streaming Media session was reset.	3
Streaming Media Session Terminated	Indicates that a Streaming Media session was terminated.	3
Streaming Media Session Denied	Indicates that a Streaming Media session was denied.	3
Streaming Media Session In Progress	Indicates that a Streaming Media session is in progress.	1
RUSERS Session Opened	Indicates that a (Remote Users) RUSERS session was established.	1
RUSERS Session Closed	Indicates that a RUSERS session was closed.	1
RUSERS Session Denied	Indicates that a RUSERS session was denied.	3
RUSERS Session In Progress	Indicates that a RUSERS session is in progress.	1
Rsh Session Opened	Indicates that a remote shell (rsh) session was established.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Rsh Session Closed	Indicates that an rsh session was closed.	1
Rsh Session Reset	Indicates that an rsh session was reset.	3
Rsh Session Terminated	Indicates that an rsh session was terminated.	3
Rsh Session Denied	Indicates that an rsh session was denied.	3
Rsh Session In Progress	Indicates that an rsh session is in progress.	1
RLOGIN Session Opened	Indicates that a Remote Login (RLOGIN) session was established.	1
RLOGIN Session Closed	Indicates that an RLOGIN session was closed.	1
RLOGIN Session Reset	Indicates that an RLOGIN session was reset.	3
RLOGIN Session Terminated	Indicates that an RLOGIN session was terminated.	3
RLOGIN Session Denied	Indicates that an RLOGIN session was denied.	3
RLOGIN Session In Progress	Indicates that an RLOGIN session is in progress.	1
REXEC Session Opened	Indicates that a (Remote Execution) REXEC session was established.	1
REXEC Session Closed	Indicates that an REXEC session was closed.	1
REXEC Session Reset	Indicates that an REXEC session was reset.	3
REXEC Session Terminated	Indicates that an REXEC session was terminated.	3
REXEC Session Denied	Indicates that an REXEC session was denied.	3
REXEC Session In Progress	Indicates that an REXEC session is in progress.	1
RPC Session Opened	Indicates that a Remote Procedure Call (RPC) session was established.	1
RPC Session Closed	Indicates that an RPC session was closed.	1
RPC Session Reset	Indicates that an RPC session was reset.	3
RPC Session Terminated	Indicates that an RPC session was terminated.	3
RPC Session Denied	Indicates that an RPC session was denied.	3

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
RPC Session In Progress	Indicates that an RPC session is in progress.	1
NTP Session Opened	Indicates that a Network Time Protocol (NTP) session was established.	1
NTP Session Closed	Indicates that an NTP session was closed.	1
NTP Session Reset	Indicates that an NTP session was reset.	3
NTP Session Terminated	Indicates that an NTP session was terminated.	3
NTP Session Denied	Indicates that an NTP session was denied.	3
NTP Session In Progress	Indicates that an NTP session is in progress.	1
NNTP Session Opened	Indicates that a Network News Transfer Protocol (NNTP) session was established.	1
NNTP Session Closed	Indicates that an NNTP session was closed.	1
NNTP Session Reset	Indicates that an NNTP session was reset.	3
NNTP Session Terminated	Indicates that an NNTP session was terminated.	3
NNTP Session Denied	Indicates that an NNTP session was denied.	3
NNTP Session In Progress	Indicates that an NNTP session is in progress.	1
NFS Session Opened	Indicates that a Network File System (NFS) session was established.	1
NFS Session Closed	Indicates that an NFS session was closed.	1
NFS Session Reset	Indicates that an NFS session was reset.	3
NFS Session Terminated	Indicates that an NFS session was terminated.	3
NFS Session Denied	Indicates that an NFS session was denied.	3
NFS Session In Progress	Indicates that an NFS session is in progress.	1
NCP Session Opened	Indicates that a Network Control Program (NCP) session was established.	1
NCP Session Closed	Indicates that an NCP session was closed.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
NCP Session Reset	Indicates that an NCP session was reset.	3
NCP Session Terminated	Indicates that an NCP session was terminated.	3
NCP Session Denied	Indicates that an NCP session was denied.	3
NCP Session In Progress	Indicates that an NCP session is in progress.	1
NetBIOS Session Opened	Indicates that a NetBIOS session was established.	1
NetBIOS Session Closed	Indicates that a NetBIOS session was closed.	1
NetBIOS Session Reset	Indicates that a NetBIOS session was reset.	3
NetBIOS Session Terminated	Indicates that a NetBIOS session was terminated.	3
NetBIOS Session Denied	Indicates that a NetBIOS session was denied.	3
NetBIOS Session In Progress	Indicates that a NetBIOS session is in progress.	1
MODBUS Session Opened	Indicates that a MODBUS session was established.	1
MODBUS Session Closed	Indicates that a MODBUS session was closed.	1
MODBUS Session Reset	Indicates that a MODBUS session was reset.	3
MODBUS Session Terminated	Indicates that a MODBUS session was terminated.	3
MODBUS Session Denied	Indicates that a MODBUS session was denied.	3
MODBUS Session In Progress	Indicates that a MODBUS session is in progress.	1
LPD Session Opened	Indicates that a Line Printer Daemon (LPD) session was established.	1
LPD Session Closed	Indicates that an LPD session was closed.	1
LPD Session Reset	Indicates that an LPD session was reset.	3
LPD Session Terminated	Indicates that an LPD session was terminated.	3
LPD Session Denied	Indicates that an LPD session was denied.	3
LPD Session In Progress	Indicates that an LPD session is in progress.	1
Lotus Notes® Session Opened	Indicates that a Lotus Notes session was established.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Lotus Notes Session Closed	Indicates that a Lotus Notes session was closed.	1
Lotus Notes Session Reset	Indicates that a Lotus Notes session was reset.	3
Lotus Notes Session Terminated	Indicates that a Lotus Notes session was terminated.	3
Lotus Notes Session Denied	Indicates that a Lotus Notes session was denied.	3
Lotus Notes Session In Progress	Indicates that a Lotus Notes session is in progress.	1
Kerberos Session Opened	Indicates that a Kerberos session was established.	1
Kerberos Session Closed	Indicates that a Kerberos session was closed.	1
Kerberos Session Reset	Indicates that a Kerberos session was reset.	3
Kerberos Session Terminated	Indicates that a Kerberos session was terminated.	3
Kerberos Session Denied	Indicates that a Kerberos session was denied.	3
Kerberos Session In Progress	Indicates that a Kerberos session is in progress.	1
IRC Session Opened	Indicates that an Internet Relay Chat (IRC) session was established.	1
IRC Session Closed	Indicates that an IRC session was closed.	1
IRC Session Reset	Indicates that an IRC session was reset.	3
IRC Session Terminated	Indicates that an IRC session was terminated.	3
IRC Session Denied	Indicates that an IRC session was denied.	3
IRC Session In Progress	Indicates that an IRC session is in progress.	1
IEC 104 Session Opened	Indicates that an IEC 104 session was established.	1
IEC 104 Session Closed	Indicates that an IEC 104 session was closed.	1
IEC 104 Session Reset	Indicates that an IEC 104 session was reset.	3
IEC 104 Session Terminated	Indicates that an IEC 104 session was terminated.	3
IEC 104 Session Denied	Indicates that an IEC 104 session was denied.	3
IEC 104 Session In Progress	Indicates that an IEC 104 session is in progress.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Ident Session Opened	Indicates that a TCP Client Identity Protocol (Ident) session was established.	1
Ident Session Closed	Indicates that an Ident session was closed.	1
Ident Session Reset	Indicates that an Ident session was reset.	3
Ident Session Terminated	Indicates that an Ident session was terminated.	3
Ident Session Denied	Indicates that an Ident session was denied.	3
Ident Session In Progress	Indicates that an Ident session is in progress.	1
ICCP Session Opened	Indicates that an Inter-Control Center Communications Protocol (ICCP) session was established.	1
ICCP Session Closed	Indicates that an ICCP session was closed.	1
ICCP Session Reset	Indicates that an ICCP session was reset.	3
ICCP Session Terminated	Indicates that an ICCP session was terminated.	3
ICCP Session Denied	Indicates that an ICCP session was denied.	3
ICCP Session In Progress	Indicates that an ICCP session is in progress.	1
GroupWiseSession Opened	Indicates that a GroupWisesession was established.	1
GroupWiseSession Closed	Indicates that a GroupWise session was closed.	1
GroupWiseSession Reset	Indicates that a GroupWisesession was reset.	3
GroupWiseSession Terminated	Indicates that a GroupWisesession was terminated.	3
GroupWiseSession Denied	Indicates that a GroupWise session was denied.	3
GroupWiseSession In Progress	Indicates that a GroupWise session is in progress.	1
Gopher Session Opened	Indicates that a Gopher session was established.	1
Gopher Session Closed	Indicates that a Gopher session was closed.	1
Gopher Session Reset	Indicates that a Gopher session was reset.	3

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Gopher Session Terminated	Indicates that a Gopher session was terminated.	3
Gopher Session Denied	Indicates that a Gopher session was denied.	3
Gopher Session In Progress	Indicates that a Gopher session is in progress.	1
GIOP Session Opened	Indicates that a General Inter-ORB Protocol (GIOP) session was established.	1
GIOP Session Closed	Indicates that a GIOP session was closed.	1
GIOP Session Reset	Indicates that a GIOP session was reset.	3
GIOP Session Terminated	Indicates that a GIOP session was terminated.	3
GIOP Session Denied	Indicates that a GIOP session was denied.	3
GIOP Session In Progress	Indicates that a GIOP session is in progress.	1
Finger Session Opened	Indicates that a Finger session was established.	1
Finger Session Closed	Indicates that a Finger session was closed.	1
Finger Session Reset	Indicates that a Finger session was reset.	3
Finger Session Terminated	Indicates that a Finger session was terminated.	3
Finger Session Denied	Indicates that a Finger session was denied.	3
Finger Session In Progress	Indicates that a Finger session is in progress.	1
Echo Session Opened	Indicates that an Echo session was established.	1
Echo Session Closed	Indicates that an Echo session was closed.	1
Echo Session Denied	Indicates that an Echo session was denied.	3
Echo Session In Progress	Indicates that an Echo session is in progress.	1
Remote .NET Session Opened	Indicates that a Remote .NET session was established.	1
Remote .NET Session Closed	Indicates that a Remote .NET session was closed.	1
Remote .NET Session Reset	Indicates that a Remote .NET session was reset.	3
Remote .NET Session Terminated	Indicates that a Remote .NET session was terminated.	3

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Remote .NET Session Denied	Indicates that a Remote .NET session was denied.	3
Remote .NET Session In Progress	Indicates that a Remote .NET session is in progress.	1
DNP3 Session Opened	Indicates that a Distributed Network Proctologic (DNP3) session was established.	1
DNP3 Session Closed	Indicates that a DNP3 session was closed.	1
DNP3 Session Reset	Indicates that a DNP3 session was reset.	3
DNP3 Session Terminated	Indicates that a DNP3 session was terminated.	3
DNP3 Session Denied	Indicates that a DNP3 session was denied.	3
DNP3 Session In Progress	Indicates that a DNP3 session is in progress.	1
Discard Session Opened	Indicates that a Discard session was established.	1
Discard Session Closed	Indicates that a Discard session was closed.	1
Discard Session Reset	Indicates that a Discard session was reset.	3
Discard Session Terminated	Indicates that a Discard session was terminated.	3
Discard Session Denied	Indicates that a Discard session was denied.	3
Discard Session In Progress	Indicates that a Discard session is in progress.	1
DHCP Session Opened	Indicates that a Dynamic Host Configuration Protocol (DHCP) session was established.	1
DHCP Session Closed	Indicates that a DHCP session was closed.	1
DHCP Session Denied	Indicates that a DHCP session was denied.	3
DHCP Session In Progress	Indicates that a DHCP session is in progress.	1
DHCP Success	Indicates that a DHCP lease was successfully obtained	1
DHCP Failure	Indicates that a DHCP lease cannot be obtained.	3
CVS Session Opened	Indicates that a Concurrent Versions System (CVS) session was established.	1
CVS Session Closed	Indicates that a CVS session was closed.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
CVS Session Reset	Indicates that a CVS session was reset.	3
CVS Session Terminated	Indicates that a CVS session was terminated.	3
CVS Session Denied	Indicates that a CVS session was denied.	3
CVS Session In Progress	Indicates that a CVS session is in progress.	1
CUPS Session Opened	Indicates that a Common UNIX Printing System (CUPS) session was established.	1
CUPS Session Closed	Indicates that a CUPS session was closed.	1
CUPS Session Reset	Indicates that a CUPS session was reset.	3
CUPS Session Terminated	Indicates that a CUPS session was terminated.	3
CUPS Session Denied	Indicates that a CUPS session was denied.	3
CUPS Session In Progress	Indicates that a CUPS session is in progress.	1
Chargen Session Started	Indicates that a Character Generator (Chargen) session was started.	1
Chargen Session Closed	Indicates that a Chargen session was closed.	1
Chargen Session Reset	Indicates that a Chargen session was reset.	3
Chargen Session Terminated	Indicates that a Chargen session was terminated.	3
Chargen Session Denied	Indicates that a Chargen session was denied.	3
Chargen Session In Progress	Indicates that a Chargen session is in progress.	1
Misc VPN	Indicates that a miscellaneous VPN session was detected	1
DAP Session Started	Indicates that a DAP session was established.	1
DAP Session Ended	Indicates that a DAP session ended.	1
DAP Session Denied	Indicates that a DAP session was denied.	3
DAP Session Status	Indicates that a DAP session status request was made.	1
DAP Session in Progress	Indicates that a DAP session is in progress.	1

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
DAP Authentication Failed	Indicates that a DAP authentication failed.	4
DAP Authentication Succeeded	Indicates that DAP authentication succeeded.	1
TOR Session Started	Indicates that a TOR session was established.	1
TOR Session Closed	Indicates that a TOR session was closed.	1
TOR Session Reset	Indicates that a TOR session was reset.	3
TOR Session Terminated	Indicates that a TOR session was terminated.	3
TOR Session Denied	Indicates that a TOR session was denied.	3
TOR Session In Progress	Indicates that a TOR session is in progress.	1
Game Session Started	Indicates that a game session was started.	1
Game Session Closed	Indicates that a game session was closed.	1
Game Session Reset	Indicates that a game session was reset.	3
Game Session Terminated	Indicates that a game session was terminated.	3
Game Session Denied	Indicates that a game session was denied.	3
Game Session In Progress	Indicates that a game session is in progress.	1
Admin Login Attempt	Indicates that an attempt to log in as an administrative user was detected.	2
User Login Attempt	Indicates that an attempt to log in as a non-administrative user was detected.	2
Client Server	Indicates client/server activity.	1
Content Delivery	Indicates content delivery activity.	1
Data Transfer	Indicates a data transfer.	3
Data Warehousing	Indicates data warehousing activity.	3
Directory Services	Indicates directory service activity.	2
File Print	Indicates file print activity.	1
File Transfer	Indicates file transfer.	2
Games	Indicates game activity.	4

Table 84. Low-level categories and severity levels for the application category (continued)

Low-level event category	Description	Severity level (0 - 10)
Healthcare	Indicates healthcare activity.	1
Inner System	Indicates inner system activity.	1
Internet Protocol	Indicates Internet Protocol activity.	1
Legacy	Indicates legacy activity.	1
Mail	Indicates mail activity.	1
Misc	Indicates miscellaneous activity.	2
Multimedia	Indicates multimedia activity.	2
Network Management	Indicates network management activity.	
P2P	Indicates Peer-to-Peer (P2P) activity.	4
Remote Access	Indicates Remote Access activity.	3
Routing Protocols	Indicates routing protocol activity.	1
Security Protocols	Indicates security protocol activity.	2
Streaming	Indicates streaming activity.	2
Uncommon Protocol	Indicates uncommon protocol activity.	3
VoIP	Indicates VoIP activity.	1
Web	Indicates web activity.	1
ICMP	Indicates ICMP activity	1

Audit

The audit category contains events that are related to audit activity, such as email or FTP activity.

The following table describes the low-level event categories and associated severity levels for the audit category.

Table 85. Low-level categories and severity levels for the audit category

Low-level event category	Description	Severity level (0 - 10)
General Audit Event	Indicates that a general audit event was started.	1
Built-in Execution	Indicates that a built-in audit task was run.	1
Bulk Copy	Indicates that a bulk copy of data was detected.	1
Data Dump	Indicates that a data dump was detected.	1

Table 85. Low-level categories and severity levels for the audit category (continued)

Low-level event category	Description	Severity level (0 - 10)
Data Import	Indicates that a data import was detected.	1
Data Selection	Indicates that a data selection process was detected.	1
Data Truncation	Indicates that the data truncation process was detected.	1
Data Update	Indicates that the data update process was detected.	1
Procedure/Trigger Execution	Indicates that the database procedure or trigger execution was detected.	1
Schema Change	Indicates that the schema for a procedure or trigger execution was altered.	1

Risk

The risk category contains events that are related to IBM Security QRadar Risk Manager.

The following table describes the low-level event categories and associated severity levels for the risk category.

Table 86. Low-level categories and severity levels for the risk category

Low-level event category	Description	Severity level (0 - 10)
Policy Exposure	Indicates that a policy exposure was detected.	5
Compliance Violation	Indicates that a compliance violation was detected.	5
Exposed Vulnerability	Indicates that the network or device has an exposed vulnerability.	9
Remote Access Vulnerability	Indicates that the network or device has a remote access vulnerability.	9
Local Access Vulnerability	Indicates that the network or device has local access vulnerability.	7
Open Wireless Access	Indicates that the network or device has open wireless access.	5
Weak Encryption	Indicates that the host or device has weak encryption.	5
Un-Encrypted Data Transfer	Indicates that a host or device is transmitting data that is not encrypted.	3
Un-Encrypted Data Store	Indicates that the data store is not encrypted.	3

Table 86. Low-level categories and severity levels for the risk category (continued)

Low-level event category	Description	Severity level (0 - 10)
Mis-Configured Rule	Indicates that a rule is not configured properly.	3
Mis-Configured Device	Indicates that a device on the network is not configured properly.	3
Mis-Configured Host	Indicates that a network host is not configured properly.	3
Data Loss Possible	Indicates that the possibility of data loss was detected.	5
Weak Authentication	Indicates that a host or device is susceptible to fraud.	5
No Password	Indicates that no password exists.	7
Fraud	Indicates that a host or device is susceptible to fraud.	7
Possible DoS Target	Indicates a host or device is a possible DoS target.	3
Possible DoS Weakness	Indicates a host or device has a possible DoS weakness.	3
Loss of Confidentiality	Indicates that a loss of confidentially was detected.	5
Policy Monitor Risk Score Accumulation	Indicates that a policy monitor risk score accumulation was detected.	1

Risk Manager Audit

The risk category contains events that are related to IBM Security QRadar Risk Manager audit events.

The following table describes the low-level event categories and associated severity levels for the Risk Manager audit category.

Table 87. Low-level categories and severity levels for the Risk Manager audit category

Low-level event category	Description	Severity level (0 - 10)
Policy Monitor	Indicates that a policy monitor was modified.	3
Topology	Indicates that a topology was modified.	3
Simulations	Indicates that a simulation was modified.	3
Administration	Indicates that administrative changes were made.	3

Control

The control category contains events that are related to your hardware system.

The following table describes the low-level event categories and associated severity levels for the control category.

Table 88. Low-level categories and severity levels for the control category

Low-level event category	Description	Severity level (0 - 10)
Device Read	Indicates that a device was read.	1
Device Communication	Indicates communication with a device.	1
Device Audit	Indicates that a device audit occurred.	1
Device Event	Indicates that a device event occurred.	1
Device Ping	Indicates that a ping action to a device occurred.	1
Device Configuration	Indicates that a device was configured.	1
Device Route	Indicates that a device route action occurred.	1
Device Import	Indicates that a device import occurred.	1
Device Information	Indicates that a device information action occurred.	1
Device Warning	Indicates that a warning was generated on a device.	1
Device Error	Indicates that an error was generated on a device.	1
Relay Event	Indicates a relay event.	1
NIC Event	Indicates a Network Interface Card (NIC) event.	1
UIQ Event	Indicates an event on a mobile device.	1
IMU Event	Indicates an event on an Integrated Management Unit (IMU).	1
Billing Event	Indicates a billing event.	1
DBMS Event	Indicates an event on the Database Management System (DBMS).	1
Import Event	Indicates that an import occurred.	1
Location Import	Indicates that a location import occurred.	1
Route Import	Indicates that a route import occurred.	1

Table 88. Low-level categories and severity levels for the control category (continued)

Low-level event category	Description	Severity level (0 - 10)
Export Event	Indicates that an export occurred.	1
Remote Signalling	Indicates remote signaling.	1
Gateway Status	Indicates gateway status.	1
Job Event	Indicates that a job occurred.	1
Security Event	Indicates that a security event occurred.	1
Device Tamper Detection	Indicates that the system detected a tamper action.	1
Time Event	Indicates that a time event occurred.	1
Suspicious Behavior	Indicates that suspicious behavior occurred.	1
Power Outage	Indicates that a power outage occurred.	1
Power Restoration	Indicates that power was restored.	1
Heartbeat	Indicates that a heartbeat ping occurred.	1
Remote Connection Event	Indicates a remote connection to the system.	1

Asset Profiler

The asset profiler category contains events that are related to asset profiles.

The following table describes the low-level event categories and associated severity levels for the asset profiler category.

Table 89. Low-level categories and severity levels for the asset profiler category

Low-level event category	Description	Severity level (0 - 10)
Asset Created	Indicates that an asset was created.	1
Asset Updated	Indicates that an asset was updated.	1
Asset Observed	Indicates that an asset was observed.	1
Asset Moved	Indicates that an asset was moved.	1
Asset Deleted	Indicates that an asset was deleted.	1
Asset Hostname Cleaned	Indicates that a host name was cleaned.	1
Asset Hostname Created	Indicates that a host name was created.	1
Asset Hostname Updated	Indicates that a host name was updated.	1

Table 89. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
Asset Hostname Observed	Indicates that a host name was observed.	1
Asset Hostname Moved	Indicates that a host name was moved.	1
Asset Hostname Deleted	Indicates that a host name was deleted.	1
Asset Port Cleaned	Indicates that a port was cleaned.	1
Asset Port Created	Indicates that a port was created.	1
Asset Port Updated	Indicates that a port was updated.	1
Asset Port Observed	Indicates that a port was observed.	1
Asset Port Moved	Indicates that a port was moved.	1
Asset Port Deleted	Indicates that a port was deleted.	1
Asset Vuln Instance Cleaned	Indicates that a vulnerability instance was cleaned.	1
Asset Vuln Instance Created	Indicates that a vulnerability instance was created.	1
Asset Vuln Instance Updated	Indicates that a vulnerability instance was updated.	1
Asset Vuln Instance Observed	Indicates that a vulnerability instance was observed.	1
Asset Vuln Instance Moved	Indicates that a vulnerability instance was moved.	1
Asset Vuln Instance Deleted	Indicates that a vulnerability instance was deleted.	1
Asset OS Cleaned	Indicates that an operating system was cleaned.	1
Asset OS Created	Indicates that an operating system was created.	1
Asset OS Updated	Indicates that an operating system was updated.	1
Asset OS Observed	Indicates that an operating system was observed.	1
Asset OS Moved	Indicates that an operating system was moved.	1
Asset OS Deleted	Indicates that an operating system was deleted.	1
Asset Property Cleaned	Indicates that a property was cleaned.	1
Asset Property Created	Indicates that a property was created.	1

Table 89. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
Asset Property Updated	Indicates that a property was updated.	1
Asset Property Observed	Indicates that a property was observed.	1
Asset Property Moved	Indicates that a property was moved.	1
Asset Property Deleted	Indicates that a property was moved.	1
Asset IP Address Cleaned	Indicates that an IP address was cleaned.	1
Asset IP Address Created	Indicates that an IP address was created.	1
Asset IP Address Updated	Indicates that an IP address was updated.	1
Asset IP Address Observed	Indicates that an IP address was observed.	1
Asset IP Address Moved	Indicates that an IP address was moved.	1
Asset IP Address Deleted	Indicates that an IP address was deleted.	1
Asset Interface Cleaned	Indicates that an interface was cleaned.	1
Asset Interface Created	Indicates that an interface was created.	1
Asset Interface Updated	Indicates that an interface was updated.	1
Asset Interface Observed	Indicates that an interface was observed.	1
Asset Interface Moved	Indicates that an interface was moved.	1
Asset Interface Merged	Indicates that an interface was merged.	1
Asset Interface Deleted	Indicates that an interface was deleted.	1
Asset User Cleaned	Indicates that a user was cleaned.	1
Asset User Observed	Indicates that a user was observed.	1
Asset User Moved	Indicates that a user was moved.	1
Asset User Deleted	Indicates that a user was deleted.	1
Asset Scanned Policy Cleaned	Indicates that a scanned policy was cleaned.	1
Asset Scanned Policy Observed	Indicates that a scanned policy was observed.	1

Table 89. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
Asset Scanned Policy Moved	Indicates that a scanned policy was moved.	1
Asset Scanned Policy Deleted	Indicates that a scanned policy was deleted.	1
Asset Windows Application Cleaned	Indicates that a Windows application was cleaned.	1
Asset Windows Application Observed	Indicates that a Windows application was observed.	1
Asset Windows Application Moved	Indicates that a Windows application was moved.	1
Asset Windows Application Deleted	Indicates that a Windows application was deleted.	1
Asset Scanned Service Cleaned	Indicates that a scanned service was cleaned.	1
Asset Scanned Service Observed	Indicates that a scanned service was observed.	1
Asset Scanned Service Moved	Indicates that a scanned service was moved.	1
Asset Scanned Service Deleted	Indicates that a scanned service was deleted.	1
Asset Windows Patch Cleaned	Indicates that a Windows patch was cleaned.	1
Asset Windows Patch Observed	Indicates that a Windows patch was observed.	1
Asset Windows Patch Moved	Indicates that a Windows patch was moved.	1
Asset Windows Patch Deleted	Indicates that a Windows patch was deleted.	1
Asset UNIX Patch Cleaned	Indicates that a UNIX patch was cleaned.	1
Asset UNIX Patch Observed	Indicates that a UNIX patch was observed.	1
Asset UNIX Patch Moved	Indicates that a UNIX patch was moved.	1
Asset UNIX Patch Deleted	Indicates that a UNIX patch was deleted.	1
Asset Patch Scan Cleaned	Indicates that a patch scan was cleaned.	1
Asset Patch Scan Created	Indicates that a patch scan was created.	1
Asset Patch Scan Moved	Indicates that a patch scan was moved.	1
Asset Patch Scan Deleted	Indicates that a patch scan was deleted.	1
Asset Port Scan Cleaned	Indicates that a port scan was cleaned.	1

Table 89. Low-level categories and severity levels for the asset profiler category (continued)

Low-level event category	Description	Severity level (0 - 10)
Asset Port Scan Created	Indicates that a port scan was cleaned.	1
Asset Port Scan Moved	Indicates that a patch scan was moved.	1
Asset Port Scan Deleted	Indicates that a patch scan was deleted.	1
Asset Client Application Cleaned	Indicates that a client application was cleaned.	1
Asset Client Application Observed	Indicates that a client application was observed.	1
Asset Client Application Moved	Indicates that a client application was moved.	1
Asset Client Application Deleted	Indicates that a client application was deleted.	1
Asset Patch Scan Observed	Indicates that a patch scan was observed.	1
Asset Port Scan Observed	Indicates that a port scan was observed.	1

Chapter 19. Ports used by QRadar

Review the common ports that are used by IBM Security QRadar, services, and components.

For example, you can determine the ports that must be opened for the QRadar Console to communicate with remote Event Processors.

Ports and iptables

The listen ports for QRadar are valid only when iptables is enabled on your QRadar system.

SSH communication on port 22

All the ports that are described in following table can be tunneled, by encryption, through port 22 over SSH. Managed hosts that use encryption can establish multiple bidirectional SSH sessions to communicate securely. These SSH sessions are initiated from the managed host to provide data to the host that needs the data in the deployment. For example, Event Processor appliances can initiate multiple SSH sessions to the QRadar Console for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. QRadar QFlow Collectors that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

QRadar ports

Unless otherwise noted, information about the assigned port number, descriptions, protocols, and the signaling direction for the port applies to all IBM Security QRadar products.

The following table lists the ports, protocols, communication direction, description, and the reason that the port is used.

Table 90. Listening ports that are used by QRadar, services, and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the QRadar Console to all other components.	Remote management access Adding a remote system as a managed host Log source protocols to retrieve files from external devices, for example the log file protocol Users who use the command-line interface to communicate from desktops to the Console High-availability (HA)
25	SMTP	TCP	From all managed hosts to the SMTP gateway	Emails from QRadar to an SMTP gateway Delivery of error and warning email messages to an administrative email contact
37	rdate (time)	UDP/TCP	All systems to the QRadar Console QRadar Console to the NTP or rdate server	Time synchronization between the QRadar Console and managed hosts
80	Apache/HTTPS	TCP	Users that connect to the QRadar Console Users that connect to the QRadar Deployment Editor	Communication and downloads from the QRadar Console to desktops The Deployment Editor application to download and show deployment information
111	Port mapper	TCP/UDP	Managed hosts that communicate to the QRadar Console Users that connect to the QRadar Console	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS)

Table 90. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. **Note:** DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
138	Windows NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter..

Table 90. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
139	Windows NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
199	NetSNMP	TCP	QRadar managed hosts that connect to the QRadar Console External log sources to QRadar Event Collectors	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console	Configuration downloads to managed hosts from the QRadar Console QRadar managed hosts that connect to the QRadar Console Users to have log in access to QRadar QRadar Console that manage and provide configuration updates WinCollect agents
445	Microsoft Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 90. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic.	External log sources to send event data to QRadar components Syslog traffic includes WinCollect agents and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the QRadar Console and NFS server	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging	Internal logging port for syslog-ng
2049	NFS	TCP	Connections between the QRadar Console and NFS server	The Network File System (NFS) protocol to share files or data between components
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QRadar QFlow Collector.	NetFlow datagram from components, such as routers
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance	Required for provisioning managed hosts from the **Admin** tab
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host Ports 7676 and 7677 are static TCP ports and four extra connections are created on random ports.

Table 90. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
7777 - 7782, 7790, 7791	JMX server ports	TCP	Internal communications, these ports are not available externally	JMX server (Mbean) monitoring for ECS, hostcontext, Tomcat, VIS, reporting, ariel, and accumulator services **Note:** These ports are used by QRadar support.
⌂7789	HA Distributed Replicated Block Device	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations
7800	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for events
7801	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for flows
7803	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Anomaly detection engine port
8000	Event Collection service (ECS)	TCP	From the Event Collector to the QRadar Console	Listening port for specific Event Collection service (ECS).
8001	SNMP daemon port	UDP	External SNMP systems that request SNMP trap information from the QRadar Console	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	None	A local port that is not used by QRadar
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector	NetFlow datagram from components, such as routers
10000	QRadar web-based, system administration interface	TCP/UDP	User desktop systems to all QRadar hosts	Server changes, such as the hosts root password and firewall access
23111	SOAP web server	TCP		SOAP web server port for the event collection service (ECS)
23333	Emulex Fibre Channel	TCP	User desktop systems that connect toQRadar appliances with a Fibre Channel card	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt)

Table 90. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
32004	Normalized event forwarding	TCP	Bidirectional between QRadar components	Normalized event data that is communicated from an off-site source or between Event Collectors
⌂32005	Data flow	TCP	Bidirectional between QRadar components	Data flow communication port between Event Collectors when on separate managed hosts
32006	Ariel queries	TCP	Bidirectional between QRadar components	Communication port between the Ariel proxy server and the Ariel query server
32009	Identity data	TCP	Bidirectional between QRadar components	Identity data that is communicated between the passive vulnerability information service (VIS) and the Event Collection service (ECS)
32010	Flow listening source port	TCP	Bidirectional between QRadar components	Flow listening port to collect data from QRadar QFlow Collectors
32011	Ariel listening port	TCP	Bidirectional between QRadar components	Ariel listening port for database searches, progress information, and other associated commands
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components	Data flows, such as events, flows, flow context, and event search queries
40799	PCAP data	TCP	From Juniper Networks SRX Series appliances to QRadar	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. **Note:** The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP)

Searching for ports in use by QRadar

Use the **netstat** command to determine which ports are in use on the QRadar Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

Procedure

1. Using SSH, log in to your QRadar Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

   ```
   netstat -nap
   ```

3. To search for specific information from the netstat port list, type the following command:

   ```
   netstat -nap | grep port
   ```

   Examples:

   - To display all ports that match 199, type the following command: `netstat -nap | grep 199`
   - To display all postgres related ports, type the following command: `netstat -nap | grep postgres`
   - To display information on all listening ports, type the following command: `netstat -nap | grep LISTEN`

Viewing IMQ port associations

You can view port numbers associations for messaging connections (IMQ) application services are allocated. To look up the additional port numbers, connect to the localhost by using telnet.

Important: Random port associations are not static port numbers. If a service is restarted, the ports that generated for a service are reallocated and the service is assigned a new set of port numbers.

Procedure

1. Using SSH to log in to the QRadar Console, as the root user.
2. To display a list of associated ports for the IMQ messaging connection, type the following command:

   ```
   telnet localhost 7676
   ```

3. If no information is displayed, press the Enter key to close the connection.

Notices

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

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

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

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

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

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

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

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

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

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

The following cross-references are used in this glossary:

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

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

A

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

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

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

anomaly
A deviation from the expected behavior of the network.

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

ARP See Address Resolution Protocol.

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

ASN See autonomous system number.

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

B

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

C

CIDR See Classless Inter-Domain Routing.

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

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

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

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

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

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

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

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

CVSS See Common Vulnerability Scoring System.

D

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

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

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

DHCP See Dynamic Host Configuration Protocol.

DNS See Domain Name System.

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

DSM See Device Support Module.

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

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

E

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

F

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

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

flow log
A collection of flow records.

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

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

FQDN
See Fully Qualified Domain Name.

FQNN
See Fully Qualified Network Name.

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

Fully Qualified Network Name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualitifed network name is CompanyA.Department.Marketing.

G

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

H

HA See high availability.

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

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

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

HMAC
See Hash-Based Message Authentication Code.

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

I

ICMP See Internet Control Message Protocol.

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

IDS See intrusion detection system.

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

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

Internet Service Provider (ISP)
An organization that provides access to the Internet.

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

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

IP See Internet Protocol.

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

IPS See intrusion prevention system.

ISP See Internet Service Provider.

L

L2L See Local To Local.

L2R See Local To Remote.

LAN See Local Area Network.

LDAP See Lightweight Directory Access Protocol.

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

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

Local Area Network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

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

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

M

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

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

N

NAT See Network Address Translation.

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

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

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

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

network object
A component of a network hierarchy.

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

O

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

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

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

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

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

OSI See Open Systems Interconnection.

OSVDB
See Open Source Vulnerability Database.

P

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

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

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

Q

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

R

R2L See Remote To Local.

R2R See Remote To Remote.

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

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

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

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

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

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

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

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

S

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

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

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

SNMP
See Simple Network Management Protocol.

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

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

subnet
See subnetwork.

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

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

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

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

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

T

TCP See Transmission Control Protocol.

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

V

violation
An act that bypasses or contravenes corporate policy.

W

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

Index

S

T

U

V

W

Printed in USA