IBM Security QRadar Log Manager
Version 7.2.0

Administration Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 237.

CONTENTS

5 SETTING UP QRADAR LOG MANAGER

6 MANAGING REFERENCE SETS

7 MANAGING BACKUP AND RECOVERY

8 USING THE DEPLOYMENT EDITOR

ABOUT THIS GUIDE

The *IBM Security QRadar Log Manager Administration Guide* provides you with information for managing QRadar Log Manager functionality requiring administrative access.

Intended audience

This guide is intended for the system administrator responsible for setting up QRadar Log Manager in your network. This guide assumes that you have QRadar Log Manager administrative access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

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

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

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

Technical documentation

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

Contacting customer support

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

Statement of good security practices

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

1 OVERVIEW

This overview includes general information on how to access and use the IBM Security QRadar Log Manager user interface and the **Admin** tab.

Supported web browsers

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

Table 1-1 Supported web browsers

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

Admin tab overview

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

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

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

- Manage users. See **User management**.
- Manage your network settings. See **Managing the system**.
- Manage high availability. See the *IBM Security QRadar High Availability Guide*.
- Manage QRadar Log Manager settings. See **Setting Up QRadar Log Manager**.

- Manage references sets. See **Managing reference sets**.
- Backup and recover your data. See **Managing backup and recovery**.
- Manage your deployment views. See **Using the deployment editor**.
- Configure syslog forwarding. See **Forwarding event data**.
- Configure plug-ins. For more information, see the associated documentation.
- 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 1-2 Admin tab menu options

Menu option	Description
Deployment Editor	Opens the Deployment Editor window. For more information, see **Using the deployment editor**.
Deploy Changes	Deploys any configuration changes from the current session to your deployment. For more information, see **Deploying changes**.
Advanced	**Deploy Full Configuration** - Deploys all configuration changes. For more information, see **Deploying changes**.

Deploying changes

When you update your configuration settings using 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 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 to allow you to scroll through the list.

The banner message also recommends which type of deployment change to make. The two options are:

- **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.

***CAUTION:** When you click **Deploy Full Configuration**, QRadar Log Manager restarts all services, which results in a gap in data collection for events 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 undeployed changes. If none are present, the following message is displayed: **`There are no changes to deploy.`**

Procedure

Step 1 Click **View Details**.

The details are displayed in groups.

Step 2 Choose one of the following options:

- To expand a group to display all items, click the plus sign (+) beside the text. When done, you can click the minus sign (-).
- To expand all groups, click **Expand All**. When done, you can click **Collapse All**.
- Click **Hide Details** to hide the details from view again.

Step 3 Perform the recommended task. Recommendations might include:

- From the **Admin** tab menu, click **Deploy Changes**.
- From the **Admin** tab menu, click **Advanced > Deploy Full Configuration**.

Updating user details

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

Procedure

Step 1 Click **Preferences**.

Step 2 Optional. Update the configurable user details:

Parameter	Description
E-mail	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 bottom right corner of the user interface. To disable popup notifications, clear this check box. For more information on the pop-up notifications, see the *IBM Security QRadar Log Manager Users Guide*.

Step 3 If you made changes, click **Save**.

Monitoring QRadar Log Manager systems with SNMP

QRadar Log Manager supports the monitoring of our appliances through SNMP polling. QRadar Log Manager uses the Net-SNMP agent, which supports a variety of system resource monitoring MIBs that can be polled by Network Management solutions for the monitoring and alerting of system resources. For more information on Net-SNMP, refer to Net-SNMP documentation.

2 USER MANAGEMENT

When you initially configure IBM Security QRadar Log Manager, you must create user accounts for all users that require access to QRadar Log Manager. 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. For each new user account you create, you must assign the following items:

- **User role** - Determines the privileges the user is granted to access functionality and information in QRadar Log Manager. QRadar Log Manager includes two default user roles: Admin and All. Before you add user accounts, you must create additional 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 Log Manager 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 additional 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.

Creating a user role

Before you can create user accounts, you must create the user roles required for your deployment. By default, QRadar Log Manager provides a default administrative user role, which provides access to all areas of QRadar Log Manager.

Before you begin

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **User Roles** icon.

Step 4 On the toolbar, click **New**.

Step 5 Configure the following parameters:

a In the **User Role Name** field, type a unique name for this user role.

b Select the permissions you want to assign to this user role. See **Table 2-1**.

Step 6 Click **Save**.

Step 7 Close the User Role Management window.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Editing a user role

You can edit an existing role to change the permissions 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, which is located above the left pane.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **User Roles** icon.

Step 4 In the left pane of the User Role Management window, select the user role you want to edit.

Step 5 On the right pane, update the permissions, as necessary. See **Table 2-1**.

Step 6 Click **Save**.

Step 7 Close the User Role Management window.

Step 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. QRadar Log Manager automatically detects this condition and prompts you to update the user accounts.

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **User Roles** icon.

Step 4 In the left pane of the User Role Management window, select the role you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 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**.

Step 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**.

Step 8 Close the User Role Management window.

Step 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 the Security Profile Management window, you can view, create, update, and delete security profiles.

Permission precedences

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

Permission precedence options include:

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

Creating a security profile

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

About this task

QRadar Log Manager 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 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Security Profiles** icon.

Step 4 On the Security Profile Management window toolbar, click **New**.

Step 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 three characters
- Maximum of 30 characters

b Optional. Type a description of the security profile. The maximum number of characters is 255.

Step 6 Click the **Permission Precedence** tab.

Step 7 In the Permission Precedence Setting pane, select a permission precedence option. See **Permission precedences**.

Step 8 Configure the networks 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 you want this security profile to have access to. Choose one of the following options:

- From the **All Networks** list box, select a network group or network.
- Select the network group or network in the navigation tree.

c Click the Add (>) icon to add the network to the Assigned Networks pane.

d Repeat for each network you want to add.

Step 9 Configure the log sources 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. Choose one of the following options:

- From the **Log Sources** list box, select a log source group or log source.
- Double-click the folder icons in the navigation tree to navigate to a specific log source group or log source.

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.

Step 10 Click **Save**.

Step 11 Close the Security Profile Management window.

Step 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, you can type the security profile name in the **Type to filter** text box, which is located above the left pane.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Security Profiles** icon.

Step 4 In the left pane, select the security profile you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters as required.

Step 7 Click **Save**.

Step 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.

Step 9 Close the Security Profile Management window.

Step 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Security Profiles** icon.

Step 4 In the left pane, select the security profile you want to duplicate.

Step 5 On the toolbar, click **Duplicate**.

Step 6 In the confirmation window, type a unique name for the duplicated security profile.

Step 7 Click **OK**.

Step 8 Update the parameters as required.

Step 9 Close the Security Profile Management window.

Step 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 Log Manager 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, which is located above the left pane.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Security Profiles** icon.

Step 4 In the left pane, select the security profile you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

If user accounts are assigned to this security profile, the **Users are Assigned to this Security Profile** window opens. Go to **Step 7**.

If no user accounts are assigned to this security profile, the security profile is successfully deleted. Go to **Step 8**.

Step 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**.

Step 8 Close the Security Profile Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

User account management

When you initially configure QRadar Log Manager, you must create user accounts for each of your users. After initial configuration, you might be required to create additional user accounts or edit 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Users** icon.

Step 4 On the User Management toolbar, click **New**.

Step 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 **E-mail** field, 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

c In the **Password** field, type a password for the user to gain access. The password must meet the following criteria:

- Minimum of five characters
- Maximum of 255 characters

d In the **Confirm Password** field, type the password again for confirmation.

e Optional. Type a description for the user account. The maximum number of characters is 2,048.

f From the **User Role** list box, select the user role you want to assign to this user.

g From the **Security Profile** list box, select the security profile you want to assign to this user.

Step 6 Click **Save**.

Step 7 Close the User Details window.

Step 8 Close the User Management window.

Step 9 On the **Admin** tab menu, click **Deploy Changes**.

Editing a user account

You can edit an existing user account.

About this task

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Users** icon.

Step 4 On the User Management window, select the user account you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update parameters, as necessary. See **Table 2-3**

Step 7 Click **Save**.

Step 8 Close the User Details window.

Step 9 Close the User Management window.

Step 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 QRadar Log Manager user interface. If the user attempts to log in to QRadar Log Manager, 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, which is located on the toolbar.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Users** icon.

Step 4 Select the user you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

Step 7 Close the User Management window.

Authentication management

You can configure authentication to validate QRadar Log Manager users and passwords. QRadar Log Manager supports various authentication types. This topic provides information and instructions for how to configure authentication.

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 using 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 on how to configure Console settings for authentication, see **Setting Up QRadar Log Manager** - **Configuring the Console settings**.

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

QRadar Log Manager supports the following user authentication types:

- **System authentication** - Users are authenticated locally by QRadar Log Manager. 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 Log Manager 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 Log Manager 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 Log Manager supports up to Cisco Secure ACS Express 4.3.
- **Active directory** - Users are authenticated by a Lightweight Directory Access Protocol (LDAP) server using Kerberos.
- **LDAP** - Users are authenticated by a Native LDAP server.

Before you begin

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

- Configure the authentication server before you configure authentication in QRadar Log Manager. See your server documentation for more information.
- Ensure the server has the appropriate user accounts and privilege levels to communicate with QRadar Log Manager. See your server documentation for more information.
- Ensure the time of the authentication server is synchronized with the time of the QRadar Log Manager server. For more information on how to set QRadar Log Manager time, see **Setting Up QRadar Log Manager**.
- Ensure all users have appropriate user accounts and roles in QRadar Log Manager to allow authentication with the vendor servers.

Configuring system authentication

You can configure local authentication on your QRadar Log Manager system.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select the **System Authentication**.

Step 5 Click **Save**.

Configuring RADIUS authentication

You can configure RADIUS authentication on your QRadar Log Manager system.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select **RADIUS Authentication**.

Step 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. The options are:

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 Log Manager uses to encrypt RADIUS passwords for transmission to the RADIUS server.

Step 6 Click **Save**.

Configuring TACACS authentication

You can configure TACACS authentication on your QRadar Log Manager system.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select **TACACS Authentication**.

Step 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. The options are:

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.
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 Log Manager uses to encrypt TACACS passwords for transmission to the TACACS server.

Step 6 Click **Save**.

Configuring Active Directory authentication

You can configure Active Directory authentication on your QRadar Log Manager system.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select **Active Directory**.

Step 5 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 domain you want to use, for example qradar.inc.

Step 6 Click **Save**.

Configuring LDAP authentication

You can configure LDAP authentication on your QRadar Log Manager system.

Before you begin

If you plan to enable the SSL connection to your LDAP server, you must import the SSL certificate from the LDAP server to the your QRadar Log Manager system. For more information on how to configure the SSL certificate, see **Configuring Your SSL certificate**.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration > User Management**.

Step 3 Click the **Authentication** icon.

Step 4 From the **Authentication Module** list box, select **LDAP**.

Step 5 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** - Enables you to search all subdirectories of the specified Directory Name (DN). • **False** - Enables you to search the immediate contents of the Base DN. The subdirectories are not searched.
LDAP User Field	Type the user field identifier 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.

Step 6 Click **Save**.

Configuring Your SSL 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

Step 1 Using SSH, log in to your system as the root user.

User Name: **root**

Password: **<password>**

Step 2 Type the following command to create the /opt/qradar/conf/trusted_certificates/ directory:

```
mkdir -p /opt/qradar/conf/trusted_certificates
```

Step 3 Copy the SSL or TLS certificate from the LDAP server to the /opt/qradar/conf/trusted_certificates directory on your QRadar Log Manager system.

Step 4 Verify that the certificate file name extension is .cert, which indicates that the certificate is trusted. QRadar Log Manager only loads `.cert` files.

User role parameters

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

Table 2-1 User Role Management window parameters

Parameter	Description
User Role Name	Type a unique name for the role. The user role name must meet the following requirements: • Minimum of three characters • Maximum of 30 characters
Admin	Select this check box to grant the user administrative access to the QRadar Log Manager 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 QRadar Log Manager. Users with this access are not able to edit other administrator accounts.

Table 2-1 User Role Management window parameters (continued)

Parameter	Description
Log Activity	Select this check box to grant the user access to all **Log Activity** tab functionality. 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 using the **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 on custom event properties, see the *IBM Security QRadar Log Manager Users Guide*. • **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 on the **Log Activity** tab, see the *IBM Security QRadar Log Manager Users Guide*.
Reports	Select this check box to grant the user access to all **Reports** tab functionality. 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 *IBM Security QRadar Log Manager Users Guide.*
IP Right Click Menu Extensions	Select this check box to grant the user access to options added to the right-click menu.

Security profile parameters

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

Table 2-2 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 three 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 2-3 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 assigned to this user account. User Roles define what actions the user has permission to perform.
Security Profile	Displays the security profile assigned to this user account. Security Profiles define what data the user has permission to access.

User management window toolbar

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

Table 2-4 User Management window toolbar functions

Function	Description
New	Click this icon to create a user account. For more information on how to create a user account, see **Creating a user account**.
Edit	Click this icon to edit the selected user account. For more information on how to edit a user account, see **Editing a user account**.

Table 2-4 User Management window toolbar functions (continued)

Function	Description
Delete	Click this icon to delete the selected user account. For more information on how to delete a user account, see **Deleting a user account**.
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

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

Table 2-5 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 five 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 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**.
Security Profile	From the list box, select the security profile 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**.

3 MANAGING THE SYSTEM

The System and License Management window provides information about each system and license in your deployment. The System and License Management window also provides options that you can use to manage your licenses, systems, and HA deployments.

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 3-1 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 the **License** option from the **Display** list box, the label on this function changes to **Allocate System to License**. For more information, see **Allocating a system to a license** or **Allocating a license to a system**.
Upload License	Use this function to upload a license to your Console. For more information, see **Uploading a license key**.

Table 3-1 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 10 days after deployment, the license state changes to **Unlocked** so that you can re-allocate 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. For more information, see **Viewing license details**. • **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**.

Table 3-1 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**. • **Add HA Host** - Select a system, and then select this option to add an HA host to the system to form an HA cluster. For more information about HA, see the *IBM Security QRadar High Availability Guide*. • **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 10 days after deployment, the license state changes to **Unlocked** so that you can re-allocate 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**. • **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**. • **Restart System** - Select a system, and then select this option to restart the system. For more information, see **Restarting a system**. • **Export Systems** - Select this option to export the listed systems to an external file that you can store on your desktop system. For more information, see **Exporting system details**.

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

Table 3-2 Deployment Details pane

Parameter	Description
Display	From this list box, select one of the following options: • **Licenses** - Displays a list of the allocated and unallocated 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 3-3 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 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 3-3 System and License Management window parameters - Systems view

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 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.
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, the System and License Management window displays the following information:

Table 3-4 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 QRadar product this license provides.

Table 3-4 System and License Management window parameters - Licenses view

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 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 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.

For your QRadar Log Manager system, a default license key provides you with access to the QRadar Log Manager 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:

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**.

3 Allocate your license. Choose one of the following options:

- **Allocating a system to a license**

- **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:

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

About this task

If you log in to QRadar Log Manager and your Console license key has 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 On the toolbar, click **Upload License**.

Step 5 In the dialog box, click **Select File**.

Step 6 On the File Upload window, locate and select the license key.

Step 7 Click **Open**.

Step 8 Click **Upload**.

Result

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

Allocating a system to a license

Each system in your deployment must be allocated a license. After you obtain and upload a license, 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

You can allocate multiple licenses to a system. For example, in addition to the QRadar Log Manager software license, you can allocate QRadar Vulnerability Manager to your Console system.

The Upload License window provides the following license details:

Table 3-5 Upload Licenses window parameters

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Licenses**.

Step 5 Select an unallocated license.

Step 6 Click **Allocate System to License**.

Step 7 Optional. To filter the list of licenses, type a keyword in the Upload License search box.

Step 8 From the list of licenses, select a license.

Step 9 Click **Allocate License to System**.

Reverting an allocation

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Licenses**.

Step 5 Select the license that you want to revert.

Step 6 Click **Actions > Revert Allocation**.

Viewing license details

A license key provides information and enforces the limits and abilities on a QRadar system. From the System and License Management window, you can view license details, such as the number of allowable log sources and the expiration dates.

About this task

The following details are available on the Current License Details window:

- Host
- Activation key
- License module
- Type
- License expiry date
- Maintenance expiry date
- Start date

- Issued date
- User limit
- Network objects limit
- Event Per Second (EPS) threshold
- Active log source limit
- Flows per interval
- Customer name (if available)
- Technical contact (if available)
- Log Manager mode
- Hardware serial number
- Offenses feature enabled

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Licenses**.

Step 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

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Licenses**.

Step 5 From the **Actions** menu, select **Export Licenses**.

Step 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.

Step 7 Click **OK**.

System management

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, restart and shut down a system, or export system details.

Viewing system details

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

About this task

The following details are available on the System Details window:

- Host name
- Host IP
- Serial number
- Version
- Appliance type
- Host status
- Event rate limit
- Flows rate limit
- License status
- License expiration date

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

Table 3-6 License parameters

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 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**.
- 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**.

Allocating a license to a system

When you install a QRadar Log Manager system, a default license key provides you with access to the QRadar Log Manager 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.

Before you begin

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

About this task

The Upload License window provides the following license details:

Table 3-7 Upload Licenses window parameters

Parameter	Description
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 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.

Table 3-7 Upload Licenses window parameters (continued)

Parameter	Description
License Expiration Date	Displays the expiration date of this license.
Event Rate Limit	Displays the event rate limit this license allows.
Flow Rate Limit	Displays the flow rate limit this license allows.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select a system.

Step 6 Click **Allocate License to System**.

Step 7 Optional. To filter the list of licenses, type a keyword in the Upload License search box.

Step 8 From the list of licenses, select a license.

Step 9 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the system that you want to restart.

Step 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the system that you want to shut down.

Step 6 From the **Actions** menu, select **Shutdown**.

Exporting system details

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 From the **Actions** menu, select **Export Systems**.

Step 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.

Step 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 *IBM Security QRadar Log Manager Installation Guide*.

Configuring firewall access

You can configure local firewall access to enable communications between devices and QRadar Log Manager. 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.

Note: 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 **Using the deployment editor**.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to configure firewall access settings.

Step 6 From the **Actions** menu, select **Manage System**.

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > Local Firewall**.

Step 9 Configure the following Device Access parameters:

Parameter	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.

Step 10 Click **Allow**.

Step 11 Configure the following 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 QRadar Log Manager 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 QRadar Log Manager user interface. Failing to do so might affect connectivity.

Step 12 Click **Allow**.

Step 13 Click **Apply Access Controls**.

Step 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 QRadar Log Manager to use and the global password for QRadar Log Manager configuration.

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to update your host setup settings.

Step 6 From the **Actions** menu, select **Manage System.**

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > QRadar Setup**.

Step 9 In the **Mail Server** field, type the address for the mail server you want QRadar Log Manager to use. QRadar Log Manager uses this mail server to distribute alerts and event messages. To use the mail server that QRadar Log Manager provides, type **localhost**.

Step 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.

Step 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to configure interface role settings.

Step 6 From the **Actions** menu, select **Manage System.**

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > Network Interfaces**.

Step 9 For each listed network interface, select the role that you want to assign to the interface from the **Role** list box.

Step 10 Click **Save Configuration**.

Step 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to configure interface role settings.

Step 6 From the **Actions** menu, select **Manage System**.

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > Root Password**.

Step 9 Update the password:

- **New Root Password** - Type the root password necessary to access the System Setup window.
- **Confirm New Root Password** - Type the password again for confirmation.

Step 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to configure system time settings.

Step 6 From the **Actions** menu, select **Manage System**.

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > System Time**.

Step 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**.

Step 10 Configure the time server:

a Click the **Time server sync** tab.

b Configure the following 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. • **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.

c 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System and License Management** icon.

Step 4 From the **Display** list box, select **Systems**.

Step 5 Select the host for which you want to configure system time settings.

Step 6 From the **Actions** menu, select **Manage System**.

Step 7 Log in to the System Setup window. The default is:

User Name: **root**

Password: **<password>**

Note: The user name and password are case sensitive.

Step 8 From the menu, select **Managed Host Config > System Time**.

Step 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.

Step 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**.

Step 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**.

Step 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**.

4 USER INFORMATION SOURCE CONFIGURATION

Configure IBM Security QRadar Log Manager to collect user and group information from Identity and Access Management endpoints. QRadar Log Manager 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 QRadar Log Manager to collect user information 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. In QRadar Log Manager, these endpoints are called user information sources.

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

- **Tivoli Directory Integrator** - For QRadar Log Manager to integrate with a user information source, you must install and configure a Tivoli Directory Integrator on a non-QRadar Log Manager host.
- **UISConfigUtil.sh** - Use this utility to create, retrieve, update, or delete user information sources. You can use user information sources to integrate QRadar Log Manager 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 QRadar Log Manager component that enables communication with an endpoint to retrieve user and group information.

QRadar Log Manager supports the following user information sources:

- **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. From Microsoft Windows AD, the following information is collected:
  - 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
- **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. From IBM Security Access Manager (ISAM), the following information is collected:
  - 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 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. From IBM Security Identity Manager (ISIM), version 6.0, the following information is collected:
  - Full name
  - DN

Reference data collections for user information

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

Consider the following example:

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

1. Create a log source to collect and parse audit data for each ISIM server from which the logs will be collected. For more information about how to create a log source, see the *IBM Security QRadar Log Source Users Guide*.
2. 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**.
3. 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 *IBM Security QRadar Log Manager Users Guide*.
4. Create an event search that uses the custom building block as a filter. For more information about event searches, see the *IBM Security QRadar Log Manager Users Guide*.
5. Create a custom report that uses the custom event search to generate daily reports on the audit activity of the privileged ISIM users. These generated reports indicate whether any ISIM administrator activity breaches your security policy. For more information about reports, see the *IBM Security QRadar Log Manager Users Guide*.

   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 integrate user and group information into QRadar Log Manager, you must configure a Tivoli Directory Integrator server, create user information sources, and collect user information from the sources.

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**.
3. Collect user information. See **Collecting user information**.

Configuring the Tivoli Directory Integrator server

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

About this task

No configuration is required on your QRadar Log Manager system; however, you must access your QRadar Log Manager 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 4-1 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

Step 1 Install Tivoli Directory Integrator on a non-QRadar Log Manager host. For more information on how to install and configure TDI, see your Tivoli Directory Integrator (TDI) documentation.

Step 2 Using SSH, log in to your Console as the root user.

User name: **`root`**

Password: **`<password>`**

Step 3 Copy the QRadarIAM_TDI.zip file to the Tivoli Directory Integrator server.

Step 4 On the Tivoli Directory Integrator server, extract the QRadarIAM_TDI.zip file in the Solutions directory.

Step 5 Configure your Tivoli Directory Integrator server to integrate with QRadar Log Manager.

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 TDI 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 TDI directory to the location from which you want to start the Tivoli Directory Integrator.

Step 6 If certificate-based authentication is required for QRadar Log Manager 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**.

Step 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 Log Manager Console.

Step 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 Log Manager Console.

Step 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 you start Tivoli Directory Integrator.*

Step 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.

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**.

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 4-2 Supported user interface property values

Property	Description
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.

Table 4-2 Supported user interface property values (continued)

Property	Description
username	Defines the user name that QRadar Log Manager 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

Step 1 Using SSH, log in to your Console as the root user.

User name: **root**

Password: **<password>**

Step 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 **Table 4-2**.

For example:

./**UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p "tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,hostname=vmibm7094.ottawa.ibm.com,port=389,username=cn=root,password=password,\"searchbase=ou=org,DC=COM\",\"searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem)(objectClass=erSystemUser))\""**

Retrieving user information sources

Use the UISConfigUtli utility to retrieve user information sources.

Procedure

Step 1 Using SSH, log in to your Console as the root user.

User name: **root**

Password: **<password>**

Step 2 Choose one of the following options:

- Type the following command to retrieve all user information sources:

  `UISConfigUtil.sh get`

- 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

Step 1 Using SSH, log in to your Console as the root user.

User name: **`root`**

Password: **`<password>`**

Step 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 **Table 4-2**.

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

Step 1 Using SSH, log in to your Console as the root user.

User name: **`root`**

Password: **`<password>`**

Step 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.

For example:

.UISConfigUtil.sh delete "UIS_AD"

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

Step 1 Using SSH, log in to your Console as the root user.

User name: **root**

Password: **<password>**

Step 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.

Result

The collected user information is stored in a reference data collection on the QRadar Log Manager 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**.

5 SETTING UP QRADAR LOG MANAGER

Using various options on the **Admin** tab, you can configure your network hierarchy, automatic updates, system settings, event retention buckets, system notifications, console settings, and index management.

Network hierarchy

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

Best practices

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

Consider the following best practices when defining your network hierarchy:

- To create a clear view of your network, group together systems and user groups that have similar behavior.
- Organize your systems and networks by role or similar traffic patterns. For example, mail servers, departmental users, labs, or development groups. This organization allows you to differentiate network behavior and enforce network management security policies.
- 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 Log Manager, allowing you to manage specific policies.
- Within a group, place servers with high volumes of traffic, such as mail servers, at the top of the group. This provides you with a clear visual representation when a discrepancy occurs.
- Do not configure a network group with more than 15 objects. Large network groups can cause you difficulty in viewing detailed information for each object.

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

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

Group	Subgroup	IP Address
Cleveland	Cleveland misc	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 new network to the above example, such as 10.10.50.0/24, which is an HR department, the traffic is displayed as Cleveland-based and any rules applied to the Cleveland group are applied by default.

Acceptable CIDR values

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

Table 5-3 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

Table 5-3 Acceptable CIDR Values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/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
/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

Defining your network hierarchy

Using the Network Views window, you can define your network hierarchy.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Network Hierarchy** icon.

Step 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.

Step 5 Click **Add**.

Step 6 Configure the following parameters:

Parameter	Description
Group	From the list box, select the group in which you want to add the new network object. If required, you can create a new group. **1** Click **Add Group**. **2** Type a unique name for the group. **3** Click **OK**.
Name	Type a unique name for the object.
Weight	Type or select the weight of the object. The range is 0 to 100 and indicates the importance of the object in the system.

Parameter	Description
IP/CIDR(s)	Type the CIDR range for this object and click **Add**. For more information on CIDR values, see **Acceptable CIDR values**.
Description	Type a description for this network object.
Color	Click **Select Color** and select a color for this object.
Database Length	From the list box, select the database length.

Step 7 Click **Save**.

Step 8 Repeat for all network objects.

Step 9 Click **Re-Order**.

Step 10 Organize the network objects as required.

Step 11 Click **Save**.

Automatic updates

You can automatically or manually update your configuration files to ensure your configuration files contain the latest network security information. QRadar Log Manager uses system configuration files to provide useful characterizations of network activity.

About automatic updates

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. For more information on setting up an automatic update server, see the **Setting up a QRadar Log Manager update server**.

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, QID map, and security threat information updates.
- DSM updates, which include corrections to parsing issues, and protocol updates.
- Major updates, which include items such as updated JAR files.
- Minor updates, which include items such as additional Online Help content or updated scripts.

QRadar Log Manager allows you to either replace your existing configuration files or integrate the updated files with your existing files to maintain the integrity of your current configuration and information.

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 on using the deployment editor, see **Using the deployment editor**.

CAUTION: *Failing to build your system and event views in the deployment editor before you configure automatic or manual updates results in your managed hosts not being updated.*

In a High Availability (HA) deployment, after you update your configuration files on a primary host and deploy your changes, the updates are automatically performed on the secondary host. If you do not deploy your changes, the updates are performed on the secondary host through an automated process that runs hourly.

Viewing pending updates

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

About this task

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 on checking for new updates, see **Checking for new updates**.

The Updates window automatically displays the Check for Updates page, which provides the following information:

Table 5-4 Check for Updates window parameters

Parameter	Description
Updates were installed	Specifies the date and time the last update was installed. If no updates have been installed, this following text is displayed: `No updates have been installed`.
Next Check for Updates	Specifies the date and time the next update is scheduled to be installed. If auto updates are disabled, the following text is displayed: `Auto Update Schedule is disabled`.
Name	Specifies the name of the update.
Type	Specifies the type of update. Types include: • DSM and protocol Updates • Minor Updates
Status	Specifies the status of the update. Status types include: • **New** - The update is not yet scheduled to be installed. • **Scheduled** - The update is scheduled to be installed. • **Installing** - The update is currently installing. • **Failed** - The updated failed to install.
Date to Install	Specifies the date on which this update is scheduled to be installed.

The Check for Updates page toolbar provides the following functions:

Table 5-5 Check for Updates Page Parameters 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**.
Install	From this list box, 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**.
Schedule	From this list box, you can configure a specific date and time to manually install selected updates on your Console. This is useful when you want to schedule the update installation during off-peak hours. For more information, see **Scheduling an update**.
Unschedule	From this list box, you can remove preconfigured schedules for manually installing updates on your Console. For more information, see **Scheduling an update**.
Search By Name	In this text box, you can type a keyword and then press Enter to 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	Click this icon to pause the automatic refresh process. To resume automatic refresh, click the **Play** icon.
Refresh	Click this icon to manually refresh the list of updates.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 To view details on an update, select the update.

Result

The description and any error messages are displayed in the right pane of the window.

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

If the **Auto Deploy** check box is clear, a system notification is displayed on the **Dashboard** tab indicating that you must deploy changes after updates are installed. By default, the check box is selected.

When the **Auto Restart Service** check box is enabled, automatic updates that require the user interface to restart is automatically performed. A user interface disruption occurs when the service restarts. When this option is disabled, updates that require your user interface to restart are prevented from automatically installing. You can manually install the updated from the Check for Updates window.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Change Settings**.

Step 5 In the Auto Update Schedule pane, configure the schedule for updates:

Parameter	Description
Frequency	From this list box, select the frequency with which you want to receive updates. Options include: • Disabled • Weekly • Monthly • Daily The default frequency is Weekly.
Hour	From this list box, select the time of day you want your system to update. The default hour is 3 am.
Week Day	This option is only available if you select **Weekly** as the update frequency. ▶ From this list box, select the day of the week you want to receive updates. The default week day is Monday.
Month Day	This option is only active when you select Monthly as the update frequency. ▶ From this list box, select the day of the month you want to receive updates. The default month day is 1.

Step 6 In the Update Types pane, configure the types of updates you want to install:

Parameter	Description
Configuration Updates	From this list box, select the method you want to use for updating your configuration files: • **Auto Integrate** - Select this option to integrate the new configuration files with your existing files and maintain the integrity of your information. This is the default setting. • **Auto Update** - Select this option to replace your existing configuration files with the new configuration files. • **Disable** - Select this option to prevent configuration updates.
DSM and Protocol Updates	From this list box, select one of the following options for DSM updates: • **Disable** - Select this option to prevent DSM and protocol updates being installed on your system. • **Manual Install** - Select this option to download the DSM and protocol updates to the designated download path location. If you choose this option, you must manually install the updates. See **Manually installing automatic updates**. • **Auto Install** - Select this option to download the DSM and protocol updates to the designated download path location and automatically install the update. This is the default setting.
Major Updates	From this list box, select one of the following options for major updates: • **Disable** - Select this option to prevent major updates being installed on your system. This is the default setting. • **Download** - Select this option to download the major updates to the designated download path location. If you choose this option, you must manually install the updates from a command line interface (CLI). See the readme file in the download files for installation instructions. ***Note:*** *Major updates cause service interruptions during installation.*
Minor Updates	From this list box, select one of the following options for minor updates: • **Disable** - Select this option to prevent minor updates being installed on your system. • **Manual Install**- Select this option to download the minor updates to the designated download path location. if you choose this option, you must manually install the updates. See **Manually installing automatic updates**. • **Auto Install** - Select this option to automatically install minor updates on your system. This is the default setting.

Step 7 Select the **Auto Deploy** check box if you want to deploy update changes automatically after updates are installed.

Step 8 Select the **Auto Restart Service** check box if you want to restart the user interface service automatically after updates are installed.

Step 9 Click the **Advanced** tab.

Step 10 In the Server Configuration pane, configure the server settings:

Parameter	Description
Web Server	Type the web server from which you want to obtain the updates. The default web server is: *http://www.ibm.com/support*
Directory	Type the directory location on which the web server stores the updates. The default directory is autoupdates/.
Proxy Server	Type the URL for the proxy server. The proxy server is only required if the application server uses a proxy server to connect to the Internet.
Proxy Port	Type the port for the proxy server. The proxy port is only required if the application server uses a proxy server to connect to the Internet.
Proxy Username	Type the user name for the proxy server. A user name is only required if you are using an authenticated proxy.
Proxy Password	Type the password for the proxy server. A password is only required if you are using an authenticated proxy.

Step 11 In the Other Settings pane, configure the update settings:

Parameter	Description
Send feedback	Select this check box if you want to send feedback to IBM regarding the update. Feedback is sent automatically using a web form when errors occur with the update. By default, this check box is clear.
Backup Retention Period (days)	Type or select the length of time, in days, that you want to store files that are replaced during the update process. The files are stored in the location specified in the **Backup Location** parameter. The default backup retention period is 30 days. The minimum is 1 day and the maximum is 65535 years.
Backup Location	Type the location where you want to store backup files.
Download Path	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.

Step 12 Click **Save**.

Scheduling an update

QRadar Log Manager performs automatic updates on a recurring schedule according to the settings on the Update Configuration page; however, if you want to schedule an update or a set of updates to run at a specific time, you can schedule an update using the Schedule the Updates window.

About this task

It is useful to schedule a large update to run during off-peak hours, thus reducing any performance impacts on your system.

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 Optional. If you want to schedule specific updates, select the updates you want to schedule.

Step 5 From the **Schedule** list box, select the type of update you want to schedule. Options include:

- All Updates
- Selected Updates
- DSM and Protocol Updates
- Minor Updates

Step 6 Using the calendar, select the start date and time of when you want to start your scheduled updates.

Step 7 Click **OK**.

Clearing scheduled updates

If required, you can clear a 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Optional. If you want to clear specific scheduled updates, select the updates you want to clear.

Step 6 From the **Unschedule** list box, select the type of scheduled update you want to clear. Options include:

- All Updates
- Selected Updates
- DSM and Protocol Updates
- Minor Updates

Step 7 Click **OK**.

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 using the **Get new updates** icon.

Before you begin

About this task

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Click **Get new updates**.

Step 6 Click **OK**.

Manually installing automatic updates

IBM provides updates on a regular basis. By default, the Auto Update feature is scheduled to automatically download and install updates. If you want to install an update at a time other than the preconfigured schedule, you can install an update using the **Install** list box on the toolbar.

About this task

The system retrieves the new updates from the Qmmunity website or *http://www.ibm.com/support. This might take an extended period of time. When complete, new updates are listed on the Updates window.*

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Check for Updates**.

Step 5 Optional. If you want to install specific updates, select the updates you want to schedule.

Step 6 From the **Install** list box, select the type of update you want to install. Options include:

- All Updates
- Selected Updates
- DSM and Protocol Updates
- Minor Updates

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:

Table 5-6 View Update History page parameters

Parameter	Description
Name	Specifies the name of the update.
Type	Specifies the type of update. Types include: • DSM and Protocol Updates • Minor Updates
Status	Specifies the status of the update. Status types include: • Installed • Failed
Installed Date	Specifies the date on which the update was installed or failed.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **View Update History**.

Step 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.

Step 6 To investigate a specific update, select the update.

Restoring hidden updates

Using the **Hide** icon, you can remove selected updates from the Check for Updates page. You can view and restore the hidden updates on the Restore Hidden Updates page.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Restore Hidden Updates**.

Step 5 Optional. To locate an update by name, type a keyword in the **Search by Name** text box and press Enter.

Step 6 Select the hidden update you want to restore.

Step 7 Click **Restore**.

Viewing the autoupdate log

The Autoupdate feature logs the most recent automatic update run on your system. You can view the Autoupdate log on the QRadar Log Manager user interface using the View Log feature.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **View Log**.

Setting up a QRadar Log Manager update server

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

About the autoupdate package

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. To receive notification of new updates, access Fix Central and click **Subscribe to notifications**.

Configuring your update server

Use this task to configure an Apache server.

Procedure

Step 1 Access your Apache server.

Step 2 Create an update directory named `autoupdates/`.

By default, the update directory is located in the web root directory of the Apache server. You can place the directory in another location if you configure QRadar Log Manager accordingly. For more information, see the *Administration Guide*.

Step 3 Optional. Create an Apache user account and password to be used by the update process.

Step 4 Download the autoupdate package from Fix Central.

a Go the Fix Central:

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

b Select **Software** > **Autoupdates**.

c Double-click the latest autoupdate package matching your QRadar Log Manager version.

d Save the file on your Apache server in the autoupdates directory.

Step 5 On the Apache server, type the following command to uncompress the autoupdate package.

```
tar -zxf updatepackage-[timestamp].tgz
```

Step 6 Configure QRadar Log Manager to accept updates:

a Click the **Admin** tab.

b On the navigation menu, click **System Configuration**.

c Click **Auto Update**.

d Click **Change Settings**.

e Select the **Advanced tab**.

f To direct the update process to the Apache server, configure the following parameters in the **Server Configuration** panel:

- **Webserver** - Type the address or directory path of the Apache server.

Note: If the Apache server runs on non-standard ports, add **`:<portnumber>`** to the end of the address. For example, https://qmmunity.q1labs.com/:8080.

- **Directory** - Type the directory location.
- **Proxy Information** - Optional. If proxy information is required to access the Apache server, configure the following parameters:
  - **Proxy Server** - Type the URL for the proxy server.
  - **Proxy Port** - Type the port for the proxy server.
  - **Proxy Username** - Type the user name for the proxy server. A user name is only required if you are using an authenticated proxy.
  - **Proxy Password** - Type the password for the proxy server. A password is only required if you are using an authenticated proxy.

g Select the **Deploy changes** check box.

h Click **Save**.

i Using SSH, log in to QRadar Log Manager as the root user.

User name: **root**

Password: **<admin password>**

j To configure the user name and password for the Apache server, type the following commands:

```
/opt/qradar/bin/UpdateConfs.pl -change_username <username>
/opt/qradar/bin/UpdateConfs.pl -change_password <password>
```

k To test your update server, type the following command:

```
lynx https://<your update server>/<directory path to updates>/manifest_list
```

l Type the user name and password.

Result

If the list of updates is not displayed, contact Customer Support.

What to do next

Adding new updates

Configuring your QRadar Log Manager Console as the Update Server

Use this task to configure your QRadar Log Manager Console as your update server.

Procedure

Step 1 Log in to QRadar Log Manager as the root user.

User name: **root**

Password: **<admin password>**

Step 2 Type the following command to create the autoupdate directory:

```
mkdir /opt/qradar/www/autoupdates/
```

Step 3 Download the autoupdate package from Fix Central.

a Go the Fix Central:

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

b Select **Software** > **Autoupdates**.

c Double-click the latest autoupdate file matching your QRadar Log Manager version.

d Save the file on your QRadar Log Manager Console in the autoupdates directory.

Step 4 On your QRadar Log Manager Console, type the following command to uncompress the autoupdate package.

```
tar -zxf updatepackage-[timestamp].tgz
```

Step 5 Configure QRadar Log Manager to accept updates:

a Log in to the QRadar Log Manager user interface.

b Click the **Admin** tab.

c On the navigation menu, click **System Configuration**.

d Click the **Auto Update** icon.

e Click **Change Settings**.

f Select the **Advanced tab**.

g In the Server Configuration pane, type **`https://localhost/`** in the **Webserver** field.

h If the **Send feedback** option in the Update Settings pane is enabled, clear the check box to disable it.

Step 6 Click **Save and Update Now**.

Adding new updates

After you have configured your update server and set up QRadar Log Manager to receive updates from the update server, adding new updates only requires you to download updates from Fix Central to your update server.

Procedure

Step 1 Download the update file from Fix Central.

a Go to Fix Central:

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

b Select **Software** > **Autoupdates**.

c Double-click the latest autoupdate package matching your QRadar Log Manager version.

d Save the file on your local update server in the directory you created when setting up your update server.

Step 2 Access your update server.

Step 3 Type the following command to uncompress the autoupdate package.

```
tar zxf <updatepackage.tgz>
```

Step 4 Log in to QRadar Log Manager as root.

Step 5 Test your update server, type the following command:

```
lynx https://<your update server>/<directory path to
updates>/manifest_list
```

Step 6 Type the user name and password of your update server.

What to do next

If the list of updates is not displayed, contact Customer Support. Configuring system settings

You can configure system settings using the System Settings window.

About this task

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

Table 5-7 System Settings window parameters

Parameter	Description
System Settings	
Administrative Email Address	Type the email address of the designated system administrator. The default email address is root@localhost.
Alert Email From Address	Type 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	Resolution interval length determines at what interval the Event Collectors sends bundles of information to the Console. From the list box, select the interval length, in minutes. The options include: • 30 seconds • 1 minute (default) • 2 minutes ***Note:*** *If you select the **30 seconds** option, results are displayed on the QRadar Log Manager 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. From the list box, select one of the following options: • **Yes** - Delete the local administrator email. This is the default setting. • **No** - Do not delete the local administrator email.
Temporary Files Retention Period	From the list box, select the period of time you want the system to retain temporary files. The default storage location for temporary files is the /store/tmp directory. The default retention period is 6 hours. The minimum is 6 hours and the maximum is 2 years.
Asset Profile Query Period	From the list box, select the period of time for an asset search to process before a time-out occurs. The default query period is 1 day. The minimum is 1 day and 1 week. ***Note:*** *This setting is only displayed if QRadar Vulnerability Manager is installed on your system.*

Table 5-7 System Settings window parameters (continued)

Parameter	Description
Coalescing Events	From the list box, select one of the following options: • **Yes** - Enables log sources to coalesce (bundle) events. • **No** - Prevents log sources from coalescing (bundling) 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 *IBM Security QRadar Managing Log Sources Guide*. The default setting is Yes.
Store Event Payload	From the list box, select one of the following options: • **Yes** - Enables log sources to store event payload information. • **No** - Prevents log sources from storing 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 *IBM Security QRadar Log Sources Users Guide*. The default setting is Yes.
Global Iptables Access	Type 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.
Syslog Event Timeout (minutes)	Type or select the amount of time, in minutes, that the status of a syslog device is recorded as error if no events have been received within the timeout period. The status is displayed on the Log Sources window (for more information, see the *IBM Security QRadar Log Sources Users Guide*). The default setting is 720 minutes (12 hours). The minimum value is zero (0) and the maximum value is 4294967294.
Partition Tester Timeout (seconds)	Type or select the amount of time, in seconds, for a partition test to perform before a time-out occurs. The default setting is 30. The minimum is zero (0) and the maximum is 4294967294. The default setting is 86400.
Max Number of TCP Syslog Connections	Type or select the maximum number of Transmission Control Protocol (TCP) syslog connections you want to allow your system. The minimum is 0 and the maximum is 4294967294. The default is 2500.
Export Directory	Type the location where event exports are stored. The default location is /store/exports.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
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	Type the location of the user profiles. The default location is /store/users.
Accumulator Retention - Minute-By-Minute	From the list box, select the period of time you want to retain minute-by-minute data accumulations. The default setting is 1 week. The minimum is 1 day and the maximum is 2 years. Every 60 seconds, the data is aggregated into a single data set.
Accumulator Retention - Hourly	From the list box, select the period of time you want to retain hourly data accumulations. The default setting is 33 days. The minimum is 1 day and the maximum is 2 years. At the end of every hour, the minute-by minute data sets are aggregated into a single hourly data set.
Accumulator Retention - Daily	From the list box, select the period of time you want to retain daily data accumulations. The default setting is 1 year. The minimum is 1 day and the maximum is 2 years. At the end of every day, the hourly data sets are aggregated into a single daily data set.
Payload Index Retention	From the list box, select the amount of time you want to store event payload indexes. The default setting is 1 week. The minimum is 1 day and the maximum is 2 years. For more information on payload indexing, see the *Enabling Payload Indexing for Quick Filtering Technical Note*.
Attacker History Retention Period	From the list box, select the amount of time that you want to store the attacker history. The default setting is 6 months. The minimum is 1 day and the maximum is 2 years.
Target Retention Period	From the list box, select the amount of time that you want to store the target history. The default setting is 6 months. The minimum is 1 day and the maximum is 2 years.
Ariel Database Settings	
Log Source Storage Location	Type the location where you want to store the log source information. The default location is /store/ariel/events. ***Note:*** *This is a global setting, applied to Consoles and managed hosts in your deployment.*
Search Results Retention Period	From the list box, select the amount of time you want to store event search results. The default setting is 1 day. The minimum is 1 day and the maximum is 3 months.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
Reporting Max Matched Results	Type or select the maximum number of results you want a report to return. This value applies to the search results on the **Log Activity**tab.The default setting is 1,000,000. The minimum value is zero (0) and the maximum value is 4294967294.
Command Line Max Matched Results	Type or select the maximum number of results you want the AQL command line to return. The default setting is 0. The minimum value is zero (0) and the maximum value is 4294967294.
Web Execution Time Limit	Type or select the maximum amount of time, in seconds, you want a query to process before a time-out occurs. This value applies to the search results on the **Log Activity** tab. The default setting is 600 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Reporting Execution Time Limit for Manual Reports	Type or select the maximum amount of time, in seconds, you want a reporting query to process before a time-out occurs. The default setting is 57600 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Command Line Execution Time Limit	Type or select the maximum amount of time, in seconds, you want a query in the AQL command line to process before a time-out occurs. The default setting is 0 seconds. The minimum value is zero (0) and the maximum value is 4294967294.
Web Last Minute (Auto refresh) Execution Time Limit	From the list box, select the maximum amount of time, in seconds, you want an auto refresh to process before a time-out occurs. The default setting is 10 seconds. The maximum is 40 seconds.
Event Log Hashing	From the list box, select one of the following options: • **Yes** - Enables QRadar Log Manager to store a hash file for every stored event log file. • **No** - Prevents QRadar Log Manager from storing a hash file for every stored event log file. The default setting is No.
HMAC Encryption	This parameter is only displayed when the **Event Log Hashing** system setting is enabled. From the list box, select one of the following options: • **Yes** - Enables QRadar Log Manager to encrypt the integrity hashes on stored event log files. • **No** - Prevents QRadar Log Manager from encrypting the integrity hashes on stored event log files. The default setting is No.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
HMAC Key	This parameter is only displayed when the **HMAC Encryption** system setting is enabled. Type the key you want to use for HMAC encryption. The maximum character length is 128 characters. The key must be unique.
Verify	This parameter is only displayed when the **HMAC Encryption** system setting is enabled. Retype the key you want to use for HMAC encryption. The key must match the key you typed in the **HMAC Key** field.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
Hashing Algorithm	You can use a hashing algorithm for database integrity. QRadar Log Manager 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 you want to use for your deployment. If the **HMAC Encryption** parameter is disabled, the following options are displayed: • **MD2** - Algorithm defined by RFC 1319. • **MD5** - Algorithm defined by RFC 1321. • **SHA-1** - Algorithm defined by Secure Hash Standard (SHS), NIST FIPS 180-1. This is the default setting. • **SHA-256** - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-256 is a 255-bit hash algorithm intended for 128 bits of security against security attacks. • **SHA-384** - Algorithm 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 defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-512 is a bit hash algorithm intended to provide 256 bits of security. If the **HMAC Encryption** parameter is enabled, the following options are displayed: • **HMAC-MD5 -** An encryption method based on the MD5 hashing algorithm. • **HMAC-SHA-1** - An encryption method based on the SHA-1 hashing algorithm. • **HMAC-SHA-256 -** An encryption method based on the SHA-256 hashing algorithm. • **HMAC-SHA-384 -** An encryption method based on the SHA-384 hashing algorithm. • **HMAC-SHA-512** An encryption method based on the SHA-512 hashing algorithm.

Table 5-7 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. From the list box, select the length of time you want the system to check for transactional issues in the database. The default setting is 10 minutes. The minimum is 1 minute and the maximum is 30 minutes.
Resolve Transaction on Non-Encrypted Host	From the list box, select whether you want the transaction sentry to resolve all error conditions 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. The default setting is Yes.
Resolve Transaction on Encrypted Host	From the list box, select whether you want the transaction sentry to resolve all error conditions 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. The default setting is Yes.
SNMP Settings	
SNMP Version	From the list box, choose one of the following options: • **Disabled** - Select this option if you do not want SNMP responses in the QRadar Log Manager custom rules engine. Disabling SNMP indicates that you do not want to accept events using SNMP. This the default. • **SNMPv3** - Select this option if you want to use SNMP version 3 in your deployment. • **SNMPv2c** - Select this option if you want to use SNMP version 2 in your deployment.
SNMPv2c Settings	
Destination Host	Type the IP address to which you want to send SNMP notifications.
Destination Port	Type the port number to which you want to send SNMP notifications. The default port is 162.
Community	Type the SNMP community, such as public.
SNMPv3 Settings	
Destination Host	Type the IP address to which you want to send SNMP notifications.
Destination Port	Type the port to which you want to send SNMP notifications. The default port is 162.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
Username	Type the name of the user you want to access SNMP related properties.
Security Level	From the list box, select the security level for SNMP. The options are: • **NOAUTH_NOPRIV** - Indicates no authorization and no privacy. This the default. • **AUTH_NOPRIV** - Indicates authorization is permitted but no privacy. • **AUTH_PRIV** - Allows authorization and privacy.
Authentication Protocol	From the list box, select the algorithm you want to use to authenticate SNMP traps.
Authentication Password	Type the password you want to use to authenticate SNMP traps.
Privacy Protocol	From the list box, select the protocol you want to use to decrypt SNMP traps.
Privacy Password	Type the password used to decrypt SNMP traps.
Embedded SNMP Daemon Settings	
Enabled	From the list box, select one of the following options: • **Yes** - Enables access to data from the SNMP Agent using SNMP requests. • **No** - Disables access to data from the SNMP Agent using SNMP requests. The default setting is Yes. After you enable the embedded SNMP daemon, you must access the host 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 Log Manager can vary depending on the vendor host. For more information on configuring your destination host to communicate with QRadar Log Manager, see your vendor documentation.
Daemon Port	Type the port you want to use for sending SNMP requests.
Community String	Type the SNMP community, such as **`public`**. This parameter only applies if you are using SNMPv2 and SNMPv3.
IP Access List	Type 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.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
IF-MAP Client/Server Settings	
IF-MAP Version	The Interface For Metadata Access Points (IF-MAP) rule response enables QRadar Log Manager to publish alert data derived from event data on an IF-MAP server. From the list box, select one of the following options: • **Disabled** - Select this option if you want to disable access to the IF-MAP Server. This is the default setting. When disabled, the other IF-MAP Client/Server settings are not displayed. • **1.1** - Select this option if you want to use IF-MAP version 1.1 in your deployment. • **2.0** - Select this option if you want to use IF-MAP version 2.0 in your deployment.
Server Address	Type the IP address of the IF-MAP server.
Basic Server Port	Type or select the port number for the basic IF-MAP server. The default port is 8443.
Credential Server Port	Type or select the port number for the credential server. The default port is 8444.
Authentication	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**. Using the list box, select the authentication type from the following options: • **Basic** - Select this option to use basic authentication. When you select this option, the **Username** and **User Password** parameters are displayed. • **Mutual** - Select this option to use mutual authentication. When you select this option, the **Key Password** parameter is displayed. The default authentication type is **Mutual**.
Key Password	This setting is displayed only when you select the **Mutual** option for the **Authentication** setting. Type the key password to be shared between the IF-MAP client and server.
Username	This setting is displayed only when you select the **Basic** option for the **Authentication** setting. Type the user name required to access the IF-MAP server.
User Password	This setting is displayed only when you select the **Basic** option for the **Authentication** setting. Type the password required to access the IF-MAP server.

Table 5-7 System Settings window parameters (continued)

Parameter	Description
Asset Profile Settings - This pane is only displayed if QRadar Vulnerability Manager is installed on your system.	
Asset Profile Retention Period	From the list box, select the period of time, in days, that you want to store the asset profile information. The default setting is **Use Advanced**. The **Use Advanced** setting enables QRadar Log Manager 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. The minimum is 1 day and the maximum is 2 years.
Enable DNS Lookups for Host Identity	From the list box, select one of the following options: • **True** - Enables QRadar Log Manager to run Domain Name System (DNS) lookups for host identity. • **False** - Prevents DNS lookups for host identity. The default setting is True.
Enable WINS Lookups for Host Identity	From the list box, select one of the following options: • **True** - Enables QRadar Log Manager to run Windows Internet Name Service (WINS) lookups for host identity. • **False** - Prevents WINS lookups for host identity. The default setting is True.
Asset Profile Reporting Interval	Type or select the interval, in seconds, that the database stores new asset profile information. The default reporting interval is 900 seconds. The minimum is zero (0) and the maximum is 4294967294.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **System Settings** icon.

Step 4 Configure the system settings. See **Table 5-7**.

Step 5 Click **Save**.

Step 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

Step 1 Using SSH, log in to QRadar Log Manager as the root user.

Username: **`root`**

Password: **`<password>`**

Step 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 QRadar Log Manager Console and your IF-MAP server. For assistance configuring the certificate on your IF-MAP server, contact your IF-MAP server administrator.

Procedure

Step 1 Using SSH, log in to QRadar Log Manager as the root user.

Username: **`root`**

Password: **`<password>`**

Step 2 Access the certificate to the /opt/qradar/conf/trusted_certificates directory

Step 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.

Step 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"
```

Step 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
```

Step 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.

Step 7 Change the permissions of the directory by typing the following commands:

```
chmod 755 /opt/qradar/conf/trusted_certificates
chmod 644 /opt/qradar/conf/trusted_certificates/*.cert
```

Step 8 Type the following command to restart the Tomcat service:

```
service tomcat restart
```

Event retention

Use the Event Retention and window available on the **Admin** tab, you can to configure custom retention periods for specific events.

About retention buckets

Each retention bucket defines a retention policy for events that match custom filter requirements. As QRadar Log Manager receives events, each event is compared against retention bucket filter criteria. When an event 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 window. 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 window provide a default retention bucket and 10 unconfigured retention buckets. Until you configure a retention bucket, all events are stored in the default retention bucket.

About this task

The Event Retention window provides the following information for each retention bucket:

Table 5-8 Retention window parameters

Parameter	Description
Order	Specifies the priority order of the retention buckets.
Name	Specifies the name of the retention bucket.
Retention	Specifies the retention period of the retention bucket.
Compression	Specifies the compression policy of the retention bucket.
Deletion Policy	Specifies the deletion policy of the retention bucket.

Table 5-8 Retention window parameters (continued)

Parameter	Description
Filters	Specifies the filters applied to the retention bucket. Move your mouse pointer over the **Filters** parameter for more information on the applied filters.
Distribution	Specifies the retention bucket usage as a percentage of total event retention in all your retention buckets.
Enabled	Specifies whether the retention bucket is enabled (true) or disabled (false). The default setting is true.
Creation Date	Specifies the date and time the retention bucket was created.
Modification Date	Specifies the date and time the retention bucket was last modified.

The Event Retention toolbars provide the following functions:

Table 5-9 Retention window toolbar

Function	Description
Edit	Click **Edit** to edit a retention bucket. For more information on editing a retention bucket, see **Editing a retention bucket**.
Enable/Disable	Click **Enable/Disable** to enable or disable a retention bucket. For more information on enabling and disabling retention buckets, see **Enabling and Disabling a Retention Bucket**.
Delete	Click **Delete** to delete a retention bucket. For more information on deleting retention buckets, see **Deleting a Retention Bucket**.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Event Retention** icon.

Step 4 Double-click the first available retention bucket.

Step 5 Configure the following parameters:

Parameter	Description
Name	Type a unique name for the retention bucket.
Keep data placed in this bucket for	From the list box, select a retention period. When the retention period is reached, events are deleted according to the **Delete data in this bucket** parameter. The default setting is 1 month. The minimum is 1 day and the maximum is 2 years.

Parameter	Description
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 events 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. The default setting is 1 week. The minimum is Never and the maximum is 2 weeks.
Delete data in this bucket	From the list box, select a deletion policy. Options include: • **When storage space is required** - Select this option if you want events that match 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. When storage is required, only events that match the Keep data placed in this bucket for parameter are deleted. • **Immediately after the retention period has expired** - Select this option if you want events to be deleted immediately on matching the **Keep data placed in this bucket for** parameter. The events are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.
Description	Type a description for the retention bucket. This field is optional.
Current Filters	In the Current Filters pane, configure your filters. To add a filter: **1** From the first list box, select a parameter you want to filter for. For example, Device, Source Port, or Event Name. **2** From the second list box, select the modifier you want to use for the filter. The list of modifiers depends on the attribute selected in the first list. **3** In the text field, type specific information related to your filter. **4** 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.

Step 6 Click **Save**.

Your event retention bucket configuration is saved.

Step 7 Click **Save**.

Your event retention bucket starts storing events that match the retention parameters immediately.

Managing retention bucket sequence

You can change the order of the retention buckets to ensure that events are 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 window. 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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Event Retention** icon.

Step 4 Select the retention bucket you want to move, and then click one of the following icons:

- **Up** - Click this icon to move the selected retention bucket up one row in priority sequence.
- **Down** - Click this icon to move the selected retention bucket down one row in priority sequence.
- **Top** - Click this icon to move the selected retention bucket to the top of the priority sequence.
- **Bottom** - Click this icon to move the selected retention bucket to the bottom of the priority sequence.

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Event Retention** icon.

Step 4 Select the retention bucket you want to edit, and then click **Edit**.

Step 5 Edit the parameters. For more information on **Table 5-8**.

Step 6 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 retention.

About this task

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Event Retention** icon.

Step 4 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 contained in the retention bucket are not removed from the system, only the criteria defining the bucket is deleted. All events are maintained in storage.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Event Retention** icon.

Step 4 Select the retention bucket you want to delete, and then click **Delete**.

Configuring system notifications

You can configure system performance alerts for thresholds using the **Admin** tab. This section provides information on configuring your system thresholds.

Before you begin

About this tasks

The following table describes the Global System Notifications window parameters

Table 5-10 Global System Notifications window parameters

Parameter	Description
System load over 1 minute	Type the threshold system load average over the last minute. The default setting is 1.8.
System load over 5 minutes	Type the threshold system load average over the last 5 minutes. The default setting is 1.5.
System load over 15 minutes	Type the threshold system load average over the last 15 minutes. The default setting is 1.3.
Percentage of swap used	Type the threshold percentage of used swap space. The default setting is 80.
Received packets per second	Type the threshold number of packets received per second. This setting is disabled by default.

Table 5-10 Global System Notifications window parameters (continued)

Parameter	Description
Transmitted packets per second	Type the threshold number of packets transmitted per second. This setting is disabled by default.
Received bytes per second	Type the threshold number of bytes received per second. This setting is disabled by default.
Transmitted bytes per second	Type the threshold number of bytes transmitted per second. This setting is disabled by default.
Receive errors	Type the threshold number of corrupted packets received per second. The default setting is 1.
Transmit errors	Type the threshold number of corrupted packets transmitted per second. The default setting is 1.
Packet collisions	Type the threshold number of collisions that occur per second while transmitting packets. The default setting is 1.
Dropped receive packets	Type the threshold number of received packets that are dropped per second due to a lack of space in the buffers. The default setting is 1.
Dropped transmit packets	Type the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers. The default setting is 1.
Transmit carrier errors	Type the threshold number of carrier errors that occur per second while transmitting packets. The default setting is 1.
Receive frame errors	Type the threshold number of frame alignment errors that occur per second on received packets. The default setting is 1.
Receive fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets. The default setting is 1.
Transmit fifo overruns	Type the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets. The default setting is 1.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Global System Notifications** icon.

Step 4 For each parameter that you want to configure:

a Enter values for the parameters. See **Table 5-10**.

b For each parameter, you must select the following options:

- **Enabled** - Select the check box to enable the option.

- **Respond if value is** - From the list box, 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.

c **Resolution Message** - Type a description of the preferred resolution to the alert.

Step 5 Click **Save**.

Step 6 On the **Admin** tab menu, click **Deploy Changes**.

Configuring the Console settings

The QRadar Log Manager Console provides the user interface for QRadar Log Manager. The Console provides real-time views, reports, and alerts. You can configure the Console to manage distributed QRadar Log Manager deployments.

About this task

The following table describes the QRadar Log Manager Console settings:

Table 5-11 QRadar Log Manager Console settings

Settings	Description
Console Settings	
ARP - Safe Interfaces	Type the interfaces you want to be excluded from ARP resolution activities.
Results Per Page	Type the maximum number of results you want to display on the main QRadar Log Manager user interface. This parameter applies to the **Log Activity** and **Reports** tabs. For example, if the **Default Page Size** parameter is configured to 50, the **Log Activity** tab displays a maximum of 50 events. The default setting is 40. The minimum is 0 and the maximum is 4294967294.
Authentication Settings	
Persistent Session Timeout (in days)	Type the length of time, in days, that a user system will be persisted. The default setting is 0, which disables this feature. The minimum is 0 and the maximum is 4294967294.
Maximum Login Failures	Type the number of times a login attempt can fail. The default setting is 5. The minimum is 0 and the maximum is 4294967294.
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. The default setting is 10 minutes. The minimum is 0 and the maximum is 4294967294.

Table 5-11 QRadar Log Manager Console settings (continued)

Settings	Description
Login Failure Block Time (in minutes)	Type the length of time that the system is locked if the maximum login failures value is exceeded. The default setting is 30 minutes. The minimum is 0 and the maximum is 4294967294.
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 will be automatically logged out of the system if no activity occurs. The default setting is 0. The minimum is 0 and the maximum is 4294967294.
Login Message File	Type the location and name of a file that includes content you want to display on the QRadar Log Manager login window. The contents of the file are displayed below the current log in window. The login message file must be located in the opt/qradar/conf directory on your system. This file might be in text or HTML format.
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 on managing users, see **User management**.
WINS Settings	
WINS Server	Type the location of the Windows Internet Naming Server (WINS) server.
Reporting Settings	
Report Retention Period	Type the period of time, in days, that you want the system to maintain reports. The default setting is 30 days. The minimum is 0 and the maximum is 4294967294.
Data Export Settings	

Table 5-11 QRadar Log Manager Console settings (continued)

Settings	Description
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. The default setting is 1. The minimum is 0 and the maximum is 4294967294.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Console** icon.

Step 4 Enter values for the parameters. See **Table 5-11**.

Step 5 Click **Save**.

Step 6 On the **Admin** tab menu, click **Deploy Changes**.

Index management

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

About indexes

Indexing event 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 properties that can be indexed and provides statistics for the properties. Toolbar options allow you to enable and disable indexing on selected event properties.

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 5-12 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. The minimum time range is **Last Hour** and the maximum time range is **Last 30 Days**. The default time range is **Last 24 Hours**. After you select a new time range option, the statistics are refreshed.
View	Allows you to display properties filtered on the **Indexed** parameter. From the list box, select one of the following options: • **All** - Displays all properties in the Index Management list. • **Enabled** - Displays only indexed properties in the Index Management list. • **Disabled** - Displays only properties that are not indexed in the Index Management list.
Database	Allows you to display properties filtered on the **Database** parameter. From the list box, select one of the following options: • **All** - Displays all properties in the Index Management list. • **Events** - Displays only event properties in the Index Management list.
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 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 Log Manager Users Guide*.
Indexed	Indicates whether the property is indexed or not: • **Green dot** - Indicates that the property is indexed. • **Empty cell** - Indicates that the property is not indexed.
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.
% 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.

Table 5-12 Index Management Window Parameters (continued)

Parameter	Description
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.

The Index Management toolbar provides the following options:

Table 5-13 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.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Index Management** icon.

Step 4 Select one or more properties from the Index Management list.

Step 5 Choose one of the following options:

- Click **Enable Index**.
- Click **Disable Index**.

Step 6 Click **Save**.

Step 7 Click **OK**.

Result

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

6 MANAGING REFERENCE SETS

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.

Reference set overview

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

After you create a reference set, you can create rules in the Rule Wizard to detect when log activity associated with the reference set occurs on your network. For example, you can create a rule to detect when a terminated user attempts to access your network resources. You can also configure a rule to add an element to a reference set when log activity matches the rule conditions. For example, you can create a rule to detect when an employee has accessed a prohibited website and add that employee's IP address to a reference set. For more information on configuring rules, see the *IBM Security QRadar Log Manager Users Guide*.

The Reference Set Management window provides the following information:

Table 6-1 Reference Set Management window parameters

Parameter	Description
Name	Displays the name of this reference set.
Number of Elements	Displays the number of elements that this reference set contains.
Type	Displays the data type of this reference set. Options include: • AlphaNumeric • Numeric • IP • Port • AlphaNumeric_Ignore_Case

Table 6-1 Reference Set Management window parameters (continued)

Parameter	Description
Associated Rules	Displays the number of rules that are configured to contribute elements to this reference set.
Capacity	Displays a visual indication of the reference set capacity used by the elements contained in the set. Reference sets can contain up to 100,000 elements.

The Reference Set Management toolbar provides the following functions:

Table 6-2 Reference Set Management toolbar functions

Function	Description
New	Click this icon to create a new reference set. See **Adding a reference set**.
Edit	Select a reference set, and then click this icon to edit the reference set. See **Editing a reference set**.
View Contents	Select a reference set, and then click this icon to view the elements and associated rules for this reference set. See **Viewing the contents of a reference set**.
Delete	Select a reference set, and then click this icon to delete the reference set. See **Deleting reference sets**.
Delete Listed	Use the **Quick Search** field to filter for specific reference sets, and then click the **Delete Listed** icon to delete these reference sets. See **Deleting reference sets**.
Quick Search	Type your keyword in the **Quick Search** field, and then click the **Quick Search** icon or press Enter on the keyboard. All reference sets that match your keyword are displayed in the Reference Set Management list. To display all reference sets again, click the eraser icon.

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 now 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.

The following table describes the New Reference Set dialog box parameters:

Table 6-3 New Reference Set dialog box parameters

Parameter	Description
Name	Type a unique name for this reference set. The maximum length is 255 characters.
Type	Using the list box, select a reference set type from the following options: • AlphaNumeric • Numeric • IP • Port • AlphaNumeric_Ignore_Case ***Note:*** *You cannot edit the* ***Type*** *parameter after you create a reference set.*
Time to Live of Elements	Using the list boxes, select the amount of time that you want to maintain each element in the reference set or select **Lives Forever**. If you specify an amount of time, you must also indicate when you want to start tracking time for an element. Select one of the following options: • Since first seen • Since last seen **Lives Forever** is the default setting.

Procedure

Step 1 On the Reference Set Management window, click **New**.

Step 2 Configure the parameters. See **Table 6-3**.

Step 3 Click **Create**.

Editing a reference set

To edit a reference set:

Procedure

Step 1 On the Reference Set Management window, select a reference set.

Step 2 Click **Edit**.

Step 3 Edit the parameters, as required. See **Table 6-3**.

Step 4 Click **Submit**.

Deleting reference sets

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

Procedure

When deleting reference sets, a confirmation window indicates if the reference sets that you want to delete have rules associated with them. After you delete a reference set, the **Add to Reference Set** configuration is cleared from the associated rules. Before you delete a reference set, you can view associated rules in the **Reference** tab. See **Viewing the contents of a reference set**.

Procedure

Step 1 Choose one of the following:

- 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**.

Step 2 Click **Delete**.

Viewing the contents of a reference set

To view the contents of a reference set:

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

Table 6-4 Content Tab Parameters

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

The **Content** tab toolbar provides the following functions:

Table 6-5 Content Tab Toolbar Functions

Function	Description
New	Click this icon to manually add an element to the reference set. See **Adding a new element to a reference set**.
Delete	Select an element, and then click this icon to delete the element.
Delete Listed	Use the **Quick Search** field to filter for specific elements, and then click the **Delete Listed** icon to delete these elements.
Import	Click this icon to import elements from a Comma-Separated Value (CSV) or text file. See **Importing elements into a reference set**.
Export	Click this icon to export the contents of this reference set to a CSV file.
Refresh Table	Click this icon to refresh the **Content** tab.
Quick Search	Type your keyword in the **Quick Search** field, and then click the **Quick Search** icon or press Enter on the keyboard. All elements that match your keyword are displayed in the Content list. To display all elements again, click the eraser icon.

The **References** tab provides a list of rules that are configured to add elements to this reference set. The **References** tab provides the following information:

Table 6-6 References tab parameters

Parameter	Description
Rule Name	Displays the name of this rule.
Group	Displays the name of the group this rule belongs to.
Category	Displays the category of this rule. Options include Custom Rule or Anomaly Detection Rule.
Type	Displays the type of this rule. Options include: Event or Common.
Enabled	Indicates whether the rule is enabled or disabled: • **true** - Indicates that this rule is enabled. • **false** - Indicates that this rule is disabled.
Response	Specifies the responses configured for this rule.
Origin	Indicates the origin of this rule. Options include: • **System** - Indicates that this is a default rule. • **Modified** - Indicates that this is a default rule that has been customized. • **User** - Indicates that this is a user-created rule.

The **References** tab toolbar provides the following functions:

Table 6-7 References tab toolbar functions

Function	Description
Edit	Click this icon to edit the rule in the Rule Wizard. You can also double-click the rule to open the Rule Wizard.
Refresh Table	Click this icon to refresh the References list.

Procedure

Step 1 On the Reference Set Management window, select a reference set.

Step 2 Click **View Contents**.

Step 3 Click the **Content** tab and view the contents. See **Table 6-4**.

Step 4 Click the **References** tab and view the references. See **Table 6-6**.

Step 5 To view or edit an associated rule, double-click the rule in the **References** list.

What to do next

In the Rule Wizard, you can edit rule configuration settings, if required.

Adding a new element to a reference set

You add a new element to a reference set using the Reference Set Management window:

Procedure

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

Step 2 Click the **Content** tab.

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

Step 4 Configure the following parameters:

Parameter	Description
Value(s)	Type the value for the element that you want to add. 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.

Step 5 Click **Add**.

Deleting elements from a reference set

You can delete elements from a reference set.

Procedure

Step 1 On the Reference Set Management window, select a reference set.

Step 2 Click **View Contents**.

Step 3 Click the **Content** tab.

Step 4 Choose one of the following:

- 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**.

Step 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

Step 1 On the Reference Set Management window, select a reference set.

Step 2 Click **View Contents**.

Step 3 Click the **Content** tab.

Step 4 On the toolbar, click **Import**.

Step 5 Click **Browse**.

Step 6 Select the CSV or text file that you want to import.

Step 7 Click **Import**.

Exporting elements from a reference set

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

Procedure

Step 1 On the Reference Set Management window, select a reference set,

Step 2 Click **View Contents**.

Step 3 Click the **Content** tab.

Step 4 On the toolbar, click **Export**.

Step 5 Choose one of the following options:

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

Step 6 Click **OK**.

7 MANAGING BACKUP AND RECOVERY

Using the Backup and Recovery feature, you can backup and recover IBM Security QRadar Log Manager configuration information and data.

Note: You can back up your event data using the Backup and Recovery feature, however, you must restore event data manually. For assistance in restoring your event data, see the *Restoring Your Data Technical Note*.

Backup and Recovery Overview

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

QRadar Log Manager enables you to perform two types of backup:

- Configuration backups, which include the following components:
  - Certificates
  - Custom logos
  - Custom rules
  - Device Support Modules (DSMs)
  - Event categories
  - Event searches
  - Groups
  - Index management information
  - License key information
  - Log sources
  - Store and Forward schedules
  - User and user roles information
  - Vulnerability data (if QRadar Vulnerability Manager is installed)
- Data backups, which include the following information:
  - Audit log information
  - Event data
  - Report data

- Indexes
- Reference set elements

Backup archive management

From this 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.

About this task

QRadar Log Manager lists all successful backup archives on the Backup Archives window, which is the first window displayed when you access the Backup and Recovery feature from the **Admin** tab.

If a backup is in progress, a status pane provides the following Information:

- **Host** - Specifies the host on which the backup is currently running.
- **Name** - Specifies the user-defined name of the backup archive.
- **Backup Type** - Specifies the type of backup that is in progress.
- **Initiated by** - Specifies the user account that initiated the backup process.
- **Initiated at** - Specifies the date and time the backup process was initiated.
- **Duration** - Specifies the elapsed time since the backup process was initiated.

Until the backup is complete, you are unable to start any new backup or restore processes.

Existing backup archives are displayed on the window. Each archive file includes the data from the previous day. The list of archives is sorted by the **Time Initiated** column in descending order. 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.

The Existing Backups pane on the Backup Archives window provides the following information for each backup archive:

Table 7-1 Existing Backups pane parameters

Parameter	Description
Host	Specifies the host that initiated the backup process.
Name	Specifies the name of the backup archive. To download the backup file, click the name of the backup.
Type	Specifies the type of backup. The options include: • **config** - Configuration data • **data** - Event data
Size	Specifies the size of the archive file.
Time Initiated	Specifies the time that the backup file was initiated.

Table 7-1 Existing Backups pane parameters (continued)

Parameter	Description
Duration	Specifies the time to complete the backup process.
Initialized By	Specifies whether the backup file was created by a user or through a scheduled process.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 On the Backup Archives window, view the list of backup archives.

Importing a backup archive

You can import a backup archive into the Existing Backups pane on your Backup Archives window. This is useful if you want to restore a backup archive that was created on another QRadar Log Manager host.

Before you begin

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 In the **Upload Archive** field, click **Browse**.

Step 5 Locate and select the archive file you want to upload. The archive file must include a .tgz extension.

Step 6 Click **Open**.

Step 7 Click **Upload**.

Deleting a backup archive

Use the Backup Archives window to delete a backup archive.

About this task

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

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 In the Existing Backups pane, select the archive you want to delete.

Step 5 Click **Delete**.

Step 6 Click **OK**.

Backup archive creation

By default, QRadar Log Manager 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. Using the Backup and Recovery feature on the **Admin** tab, you can customize this nightly backup and create an on-demand configuration backup, as required.

Configuring your scheduled 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 Log Manager processes.

The Backup Recovery Configuration window provides the following parameters:

Table 7-2 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. ***Note:*** *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 Log Manager deployment. For more information on using NFS, see the Configuring 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 one of the following options: • **No Nightly Backups** - Disables the nightly scheduled backup process. • **Configuration Backup Only** - Enables a nightly backup archive that includes configuration information only. This is the default option. • **Configuration and Data Backups** - Enables a nightly backup that includes configuration information and data.
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.

Table 7-2 Backup Recovery Configuration parameters (continued)

Parameter	Description
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. Options include: • LOW • MEDIUM • HIGH 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 box, select the level of importance you want the system to place on the data backup process compared to other processes. Options include: • LOW • MEDIUM • HIGH A priority of medium or high have a greater impact on system performance.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 On the toolbar, click **Configure**.

Step 5 On the Backup Recovery Configuration window, customize your nightly backup. See **Table 7-2**.

Step 6 Click **Save**.

Step 7 Close the Backup Archives window.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Creating an on-demand configuration backup archive

To backup 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

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

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 From the toolbar, click **On Demand Backup**.

Step 5 Enter values for the following parameters:

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

Step 6 Click **Run Backup**.

Step 7 Click **OK**.

Result

Until the on-demand backup is complete, you are unable to start any new backup or restore processes. You can monitor the backup archive process in the Backup Archives window. See **Table 7-1**.

Backup archive restoration

Using the Restore a Backup window, you can restore a backup archive. This is useful if you want to restore previously archived configuration files on your QRadar Log Manager system.

Restoring a backup archive

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

Before you begin

Before you begin, 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 Log Manager 7.1.0 (MR2), the backup archive must have been created in IBM Security QRadar Log Manager 7.1.0 (MR2).
- The restore process only restores your configuration information. For assistance in restoring your event 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.

About this task

Do not restart the Console until the restore process is complete. During the restore process, the following steps are taken on the Console:

- Existing files and database tables are backed up.
- Tomcat is shut down.
- All system processes are shut down.
- Files are extracted from the backup archive and restored to disk.
- Database tables are restored.
- All system processes are restarted.
- Tomcat restarts.

The restore process can take up to several hours depending on the size of the backup archive being 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 Restore a Backup window provides the following parameters:

Table 7-3 Restore a Backup Window Parameters

Parameter	Description
Name	Displays the name of the backup archive.
Description	Displays the description, if any, of the backup archive.
Type	Specifies 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.

Table 7-3 Restore a Backup Window Parameters (continued)

Parameter	Description
Restore Configuration	The Restore Configuration pane 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. Options include: • Custom Rules Configuration • Deployment Configuration, which includes: Certificates Custom logos Device Support Modules (DSMs) Event categories Event searches Groups Index management information Log sources Store and Forward schedules Vulnerability data (if QRadar Vulnerability Manager is installed) • User and user roles information • License key information
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.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 Select the archive you want to restore.

Step 5 Click **Restore**.

Step 6 On the Restore a Backup window, configure the parameters, as required. See **Table 7-3**.

Step 7 Click **Restore**.

Step 8 Click **OK**.

Step 9 Click **OK**.

Step 10 Choose one of the following options:

- If the QRadar Log Manager user interface was closed during the restore process, open a browser and log in to QRadar Log Manager.
- If the QRadar Log Manager user interface has not been closed, the login window is displayed. Log in to QRadar Log Manager.

Step 11 Follow the instructions on the status window.

What to do next

After you have verified that your data is restored to your system, you must re-apply RPMs for any DSMs, 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 backup was performed, the secondary host displays a Failed status on the System and License Management window.

Restoring a backup archive created on a different QRadar Log Manager system

Each backup archive includes IP address information of the system from which the backup archive was created. When restoring a backup archive from a different QRadar Log Manager system, the IP address of the backup archive and the system you are restoring the backup are mismatched. This procedure provides steps to correct this.

About this task

Do not restart the Console until the restore process is complete. During the restore process, the following steps are taken on the Console:

- Existing files and database tables are backed up.
- Tomcat is shut down.
- All system processes are shut down.
- Files are extracted from the backup archive and restored to disk.
- Database tables are restored.
- All system processes are restarted.
- Tomcat restarts.

The restore process can take up to several hours depending on the size of the backup archive being 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 Restore a Backup window includes a message asking you to 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 7-4 Restore a Backup (Managed Host Accessibility) parameters

Parameter	Description
Host Name	Specifies the managed host name.
IP Address	Specifies the IP address of the managed host.
Access Status	Specifies the access status to the managed host. The options include: • **Testing Access** - Specifies the test to determine access status is not complete. • **No Access** - Specifies the managed host cannot be accessed. • **OK** - Specifies the managed host is accessible.

The Restore a Backup window provides the following parameters:

Table 7-5 Restore a Backup window parameters

Parameter	Description
Name	Displays the name of the backup archive.
Description	Displays the description, if any, of the backup archive.
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 this check box.

Table 7-5 Restore a Backup window parameters (continued)

Parameter	Description
Restore Configuration	The Restore Configuration pane 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. Options include: • Custom Rules Configuration • Deployment Configuration, which includes: Custom logos Device Support Modules (DSMs) Event categories Event searches Groups Log sources Certificates • User and user roles information • License key information
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 the check box.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Backup and Recovery** icon.

Step 4 Select the archive you want to restore.

Step 5 Click **Restore**.

Step 6 Stop IP tables:

a Using SSH, log into the managed host as the root user.

User Name: **root**

Password: **<password>**

b Type the following command:

```
service iptables stop
```

c Repeat for all managed hosts in your deployment.

Step 7 On the Restore a Backup window, click **Test Hosts Access**.

Step 8 After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**. See **Table 7-4**.

Step 9 If the **Access Status** column indicates a status of **No Access** for a host, stop iptables (see **Step 6**) again, and then click **Test Host Access** again to attempt a connection.

Step 10 On the Restore a Backup window, configure the parameters. See **Table 7-5**.

Step 11 Click **Restore**.

Step 12 Click **OK**.

Step 13 Click **OK** to log in. Choose one of the following options:

- If the QRadar Log Manager user interface has been closed during the restore process, open a browser and log in to QRadar Log Manager.
- If the QRadar Log Manager user interface has not been closed, the login window is automatically displayed. Log in to QRadar Log Manager.

Step 14 View the results of the restore process and follow the instructions to resolve errors, if required.

Step 15 Refresh your browser window.

Step 16 From the **Admin** tab, select **Advanced > Deploy Full Configuration**.

What to do next

After you have verified that your data is restored to your system, you must re-apply RPMs for any DSMs, or log source protocols.

If the backup archive originated on an HA cluster and 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 backup was performed, the secondary host displays a **Failed** status on the System and License Management window.

8 USING THE DEPLOYMENT EDITOR

Using the deployment editor, you can manage the individual components of your IBM Security QRadar Log Manager deployment. After you configure your deployment, you can access and configure the individual components of each managed host in your deployment.

Deployment editor requirements

The deployment editor requires Java™ Runtime Environment (JRE). You can download Java™ 1.6 or 1.7 at the following website: *http://www.java.com*. Also, 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 or MyIE, install components that might be incompatible with the **Admin** tab. You might be required to disable any Web browsers installed on your system. For further assistance, contact Customer Support.

To access the deployment editor from behind a proxy server or firewall, you must configure the appropriate proxy settings on your desktop. This allows the software to automatically detect the proxy settings from your browser.

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

About the deployment editor user interface

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

The deployment editor provides the following views of your deployment:

- **System View** - Use the System View page to assign software components, such as a QFlow Collector, 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 Log Manager software installed. By default, the System View page also includes the following components:
  - **Host Context** - Monitors all QRadar Log Manager components to ensure that each component is operating as expected.
  - **Accumulator** - Analyzes events, reporting, writing database data, and alerting a DSM. An accumulator resides on any host that contains an Event Processor.
- **Event View** - Use the Event View page to create a view of your components including QFlow Collectors, Event Processors, Event Collectors, Off-site Sources, Off-site Targets, and Magistrate components.
- **Vulnerability View** - Use the Vulnerability View page to create a view of your QRadar Vulnerability Manager components. This page is only displayed when you have installed and licensed IBM Security QRadar Vulnerability Manager. For more information, see the *IBM Security IBM Security QRadar Vulnerability Manager Users Guide*.

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

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 re-assigned to another host. Also, if you add a managed host to your deployment, the deployment editor displays a message indicating that the managed host has been added.

Menu options

The displayed menu options depend on the selected component in your view. The following table provides a list of the menu options:

Table 8-1 Deployment editor menu options

Menu Option	Sub Menu Option	Description
File	Save to staging	Saves deployment to the staging area.
	Save and close	Saves deployment to the staging area and closes the deployment editor.
	Open staged deployment	Opens a deployment that was previously saved to the staging area.
	Open production deployment	Opens a deployment that was previously saved.
	Close current deployment	Closes the current deployment.
	Revert	Reverts current deployment to the previously saved deployment.
	Edit Preferences	Opens the Deployment Editor Settings window.
	Close editor	Closes the deployment editor.
Edit	Delete	Deletes a component, host, or connection.
Actions	Add a managed host	Opens the Add a Managed Host wizard.
	Manage NATed Networks	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
	Rename component	Renames an existing component. This option is only available when a component is selected.
	Configure	Configures QRadar Log Manager components. This option is only available when a QFlow Collector, Event Collector, Event Processor, or Magistrate is selected.
	Assign	Assigns a component to a managed host. This option is only available when a QFlow Collector, Event Collector, Event Processor, or Magistrate is selected.
	Unassign	Unassigns a component from a managed host. This option is only available when a QFlow Collector is selected. The host for the selected component must be running the version of QRadar Log Manager software as the managed host.

Toolbar functions

The deployment editor provides the following toolbar functions:

Table 8-2 Toolbar functions

Function	Description
Save and Close	Saves deployment to the staging area and closes the deployment editor.
Open Current Deployment	Opens current production deployment.
Open Staged Deployment	Opens a deployment that was previously saved to the staging area.
Discard	Discards recent changes and reloads last saved model.
Remove	Deletes selected item from the deployment view. This option is only available when the selected component has a managed host running a compatible version of QRadar Log Manager software.
Add Managed Host	Opens the Add a Managed Host wizard, which allows you to add a managed host to your deployment.
Manage NATed Networks	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
Reset the zoom	Resets the zoom to the default.
Zoom in	Zooms in.
Zoom Out	Zooms out.

Configuring deployment editor preferences

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

Procedure

Step 1 Select **File > Edit Preferences**.

Step 2 Configure the following parameters:

- **Presence Poll Frequency** - Type how often, in milliseconds, you want the managed host to monitor your deployment for updates, for example, a new or updated managed host.
- **Zoom Increment** - Type the increment value when the zoom option is selected. For example. 0.1 indicates 10%.

Building your deployment

Using the deployment editor and options on the **Admin** tab, you can build and deploy your deployment.

Before you Begin

Before you begin, you must:

- Install the Java™ Runtime Environment (JRE). You can download Java 1.6 or 1.7 at the following website: *http://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 Log Manager deployment, including the IP addresses and login information for all devices in your QRadar Log Manager deployment.

Note: If you require assistance, contact Customer Support.

To build your deployment, you must perform the following tasks:

1. Build your Event View. See **Event view management**.
2. Build your System View. See **System view management**.
3. Configure components. See **Component configuration**.
4. Stage your deployment change. From the deployment editor menu, select **File > Save to Staging**.
5. Deploy all configuration changes. On the **Admin** tab menu, select **Advanced > Deploy Changes**.

Event view management

The Event View page allows you to create and manage the components for your deployment.

QRadar Log Manager components

QRadar Log Manager includes the following deployment components:

- **Event Collector** - Collects security events from various types of security devices, 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 virtually identical events to conserve system usage.
- **Event Processor** - An Event Processor processes event data from the Event Collector. The events are bundled to conserve network usage. When received, the Event Processor correlates the information from QRadar Log Manager and distributes to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by QRadar Log Manager to indicate any behavioral changes or policy violations for that event. Rules are then applied to the events that allow the Event Processor to process according to the configured rules. When complete, the Event Processor sends the events to the Magistrate.

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

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

QRadar Log Manager deployment that includes SIEM components.

- **Off-site Source** - Indicates an off-site event data source that forwards normalized data to an Event Collector. You can configure an off-site source to receive events and allows the data to be encrypted before forwarding.
- **Off-site Target** - Indicates an off-site device that receives event data. An off-site target can only receive data from an Event Collector.
- **Magistrate** - The Magistrate component provides the core processing components of the security information and event management (SIEM) 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 against the defined custom rules to create an event. If no custom rules exist, the Magistrate uses the default rule set to process the offending alert event. An alert event is an event that has been processed through QRadar Log Manager using multiple inputs, individual events, and combined events with analyzed behavior and vulnerabilities.

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

To build your Event View:

1. Add SIEM components to your view. See **Adding components**.
2. Connect the components. See **Connecting components**.
3. Connect deployments. See **Forwarding normalized events**.
4. Rename the components so each component has a unique name. See **Renaming components**.

Adding components

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

About this task

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

- Event Collector
- Event Processor
- Off-site Source
- Off-site Target
- QFlow Collector

Procedure

Step 1 On the **Admin** tab, click **Deployment Editor**.

Step 2 In the Event Components pane, select a component you want to add to your deployment.

Step 3 Type a unique name for the component you want to add. The name can be up to 20 characters in length and might include underscores or hyphens. Click **Next**.

Step 4 From the **Select a host to assign to** list box, select a managed host you want to assign the new component to. Click **Next**.

Step 5 Click **Finish**.

Step 6 Repeat for each component you want to add to your view.

Step 7 From the deployment editor menu, select **File > Save to staging**.

The deployment editor saves your changes to the staging area and automatically closes.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

What to do next

You must connect the components you added to your deployment. See **Connecting components**.

Connecting components

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

Before you begin

You must add components to your deployment. See **Adding components**.

About this task

The Event View page only allows you to connect appropriate components together. For example, you can connect an Event Collector to an Event Processor, but not a Magistrate component.

The following table provides a list of components you are able to connect.

Table 8-3 Component connections

You can connect a...	To	Connection guide
QFlow Collector	Event Collector	• A QFlow Collector can only be connected to an Event Collector. • The number of connections is not restricted.
Event Collector	Event Processor	• An Event Collector can only be connected to one Event Processor. • A Console Event Collector can only be connected 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 already 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.
Event Processor	Magistrate (MPC)	Only one Event Processor can connect to a Magistrate.
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

Step 1 In the Event View page, select the component for which you want to establish a connection.

Step 2 From the menu, select **Actions > Add Connection**.

An arrow is displayed in your map. The arrow represents a connection between two components.

Step 3 Drag the end of the arrow to the component you want to establish a connection to.

Step 4 Repeat for all remaining components that require connections.

What to do next

You must configure your deployment to forward normalized events. See **Forwarding normalized events**.

Forwarding normalized events

To forward normalized events, you must configure an off-site Event Collector (target) in your current deployment to receive events from an associated off-site Event Collector in the receiving deployment (source).

Before you begin

You must connect the components to your deployment. See **Connecting components**.

About this task

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

- **Off-site Source** - An off-site Event Collector from which you want to receive event data. The off-site source must be configured with appropriate permissions to send event data to the off-site target.
- **Off-site Target** - An off-site Event Collector to which you want to send event data.

Example

To forward normalized events between two deployments (A and B), where deployment B wants to receive events 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, if you want to enable encryption between the off-site source and Event Collector B, you must copy the public key (located at /root/.ssh/id_rsa.pub) from

the off-site source to Event Collector B (add the contents of the file to /root/.ssh/authorized_keys).

Note: 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 on 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

Step 1 On the **Admin** tab, click **Deployment Editor**.

Step 2 In the Event Components pane, select one of the following options:

- **Off-site Source**
- **Off-site Target**

Step 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**.

Step 4 Enter values for the parameters:

- **Enter a name for the off-site host** - Type the name of the off-site host. The name can be up to 20 characters in length and might include the underscores or hyphens characters.
- **Enter the IP address of the source server** - Type the IP address of the managed host you want to connect the off-site host to.
- **Receive Events** - Select the check box to enable the off-site host to receive events.
- **Encrypt traffic from off-site source** - Select the check box to encrypt traffic from an off-site source. When enabling encryption, you must select this check box on the associated off-site source and target.

Step 5 Click **Next**.

Step 6 Click **Finish**.

Step 7 Repeat for all remaining off-site sources and targets.

Step 8 From the deployment editor menu, select **File > Save to staging**.

Step 9 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

What to do next

You must rename the components in your Event View to uniquely identify components throughout your deployment. See **Renaming components**.

Renaming components

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

Before you begin

You must add components to your deployment. See **Adding components**.

Procedure

Step 1 In the Event Components pane, select the component you want to rename.

Step 2 From the menu, select **Actions > Rename Component**.

Step 3 Type a new name for the component. The name must be alphanumeric with no special characters.

Step 4 Click **OK**.

System view management

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

About the System View page

The System View page allows you to manage all managed hosts in your network.

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

Using the System View page, you can perform the following tasks:

- Add managed hosts to your deployment. See **Adding a managed host**.
- Use QRadar Log Manager with NATed networks in your deployment. See **NAT management**.
- Update the managed host port configuration. See **Configuring a managed host**.
- Assign a component to a managed host. See **Assigning a component to a host**.
- Configure Host Context. See **Configuring Host Context**.
- Configure an Accumulator. See **Configuring an accumulator**.

Software version requirements

You cannot add, assign or configure components on a non-Console managed host when the QRadar Log Manager software version is incompatible with the software version that the Console is running. If a managed host has previously assigned components and is running an incompatible software version, you can still view the components, however, you are not able to update or delete the components. For more information, contact Customer Support.

Encryption

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

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

CAUTION: *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

Before you add a managed host, make sure the managed host includes QRadar Log Manager software.

About this task

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see **NAT management**.

If you want to add a non-NATed managed host to your deployment when the Console is NATed, you must change the Console to a NATed host (see **Changing the NAT status for a Managed Host**) before adding the managed host to your deployment.

Procedure

Step 1 From the menu, select **Actions > Add a Managed Host**.

Step 2 Click **Next**.

Step 3 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of the host you want to add to your System View.
- **Enter the root password of the host** - Type the root password for the host.
- **Confirm the root password of the host** - Type the password again.
- **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.
- **Enable Compression** - Select the check box to enable data compression between two managed hosts.

If you selected the Host is NATed check box, the Configure NAT Settings page is displayed. Go to **Step 4**. Otherwise, go to **Step 5**.

Step 4 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use.
  - If the managed host is on the same subnet as the Console, select the Console of the NATed network.
  - If the managed host is not on the same subnet as the Console, select the managed host of the NATed network.

Step 5 Click **Next**.

Step 6 Click **Finish**.

What to do next

If your deployment included undeployed changes, a window is displayed requesting you to deploy all changes.

Editing a managed host

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

About this task

If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see **NAT management**.

If you want to add a non-NATed managed host to your deployment when the Console is NATed, you must change the Console to a NATed host (see **Changing the NAT status for a Managed Host**) before adding the managed host to your deployment.

Procedure

Step 1 Click the **System View** tab.

Step 2 Right-click the managed host you want to edit and select **Edit Managed Host**.

Note: This option is only available when the selected component has a managed host running a compatible version of QRadar Log Manager software.

Step 3 Click **Next**.

Step 4 Edit the following values, as necessary:

- **Host is NATed** - Select the check box if you want to use existing Network Address Translation (NAT) on this managed host.
- **Enable Encryption** - Select the check box if you want to create an encryption tunnel for the host.

If you selected the Host is NATed check box, the Configure NAT settings page is displayed. Go to **Step 5**. Otherwise, go to **Step 6**.

Step 5 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use.

Step 6 Click **Next**.

Step 7 Click **Finish**.

Removing a managed host

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

About this task

The **Remove host** option is only available when the selected component has a managed host running a compatible version of QRadar Log Manager software.

Procedure

Step 1 Click the **System View** tab.

Step 2 Right-click the managed host you want to delete and select **Remove host**.

Step 3 Click **OK**.

Step 4 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Configuring a managed host

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

Procedure

Step 1 From the System View page, right-click the managed host you want to configure and select **Configure**.

Step 2 Enter values for the parameters:

- **Minimum port allowed** - Type the minimum port for which you want to establish communications.
- **Maximum port allowed** - Type the maximum port for which you want to establish communications.
- **Ports to exclude** - Type the ports you want to exclude from communications. Separate multiple ports using a comma.

Step 3 Click **Save**.

Assigning a component to a host

You can use the System View page to assign the QRadar Log Manager components that you added in the Event View page to the managed hosts in your deployment.

About this task

The list box only displays managed hosts that are running a compatible version of QRadar Log Manager software.

Procedure

Step 1 Click the **System View** tab.

Step 2 From the **Managed Host** list, select the managed host you want to assign a QRadar Log Manager component to.

Step 3 Select the component you want to assign to a managed host.

Step 4 From the menu, select **Actions > Assign**.

Step 5 From the **Select a host** list box, select the host that you want to assign to this component. Click **Next**.

Step 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.

About this task

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

The following table describes the Host Context parameters:

Table 8-4 Host Context parameters

Parameter	Description
Disk Usage Sentinel Settings	
Warning Threshold	When the configured threshold of disk usage is exceeded, an email is sent to the administrator indicating the current state of disk usage. The default warning threshold is 0.75, therefore, when disk usage exceeds 75%, an email is sent indicating that disk usage is exceeding 75%. 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 Type the warning threshold for disk usage. ***Note:*** *Notification emails are sent from the email address 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* **Setting Up QRadar Log Manager***.*
Recovery Threshold	When the system has exceeded 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%. Type the recovery threshold. ***Note:*** *Notification emails are sent from the email address 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* **Setting Up QRadar Log Manager***.*
Shutdown Threshold	When the system exceeds the shutdown threshold, all processes are stopped. An email is sent to the administrator indicating the current state of the system. The default is 0.95, therefore, when disk usage exceeds 95%, all processes stop. Type the shutdown threshold. ***Note:*** *Notification emails are sent from the email address 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* **Setting Up QRadar Log Manager***.*

Table 8-4 Host Context parameters (continued)

Parameter	Description
Inspection Interval	Type the frequency, in milliseconds, that you want to determine disk usage.
SAR Sentinel Settings	
Inspection Interval	Type the frequency, in milliseconds, that you want to inspect SAR output. The default is 300,000 ms.
Alert Interval	Type the frequency, in milliseconds, that you want to be notified that the thresholds have been exceeded. The default is 7,200,000 ms.
Time Resolution	Type the time, in seconds, that you want the SAR inspection to be engaged. The default is 60 seconds.
Log Monitor Settings	
Inspection Interval	Type the frequency, in milliseconds, that you want to monitor the log files. The default is 60,000 ms.
Monitored SYSLOG File Name	Type a filename for the SYSLOG file. The default is /var/log/qradar.error.
Alert Size	Type the maximum number of lines you want to monitor from the log file. The default is 1000.

Procedure

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Select the managed host that includes the host context you want to configure.

Step 3 Select the Host Context component.

Step 4 From the menu, select **Actions > Configure**.

Step 5 Enter values for the parameters. See **Table 8-4**.

Step 6 Click **Save**.

Configuring an accumulator

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

About this task

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 events from the local Event Processor, writing database data, and contains the Anomaly Detection Engine (ADE).

The Accumulator Configuration window provides the following parameters.

Table 8-5 Accumulator parameters

Parameter	Description
Central Accumulator	Specifies if the current component is a central accumulator. A central accumulator only exists on a Console system. Options include: • **True** - Specifies that the component is a central accumulator on the Console and receives TCP data from non-central accumulators. • **False** - Specifies that the component is not a central accumulator, but is deployed on the Event Processor and forwards data to a central accumulator on the Console.
Anomaly Detection Engine	Type the address and port of the ADE. The 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	Type the listen port of the accumulator responsible for receiving streams of events from the event processor. The default value is 7802.
Alerts DSM Address	Type the DSM address for forwarding alerts from the accumulator using the following syntax: **<DSM_IP address>:<DSM port number>**.

Procedure

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Select the managed host you want to configure.

Step 3 Select the accumulator component.

Step 4 From the menu, select **Actions > Configure**.

Step 5 Configure the parameters. See **Table 8-5**.

Step 6 Click **Save**.

NAT management

Using the deployment editor, you can manage NAT'd deployments.

About NAT

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 essentially hides internal IP addresses.

You can add a non-NATed managed host using inbound NAT for a public IP address. You can also use a dynamic IP address for outbound NAT. However, both must be located 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 adding or editing a managed host, you can enable NAT for that managed host. You can also use the deployment editor to manage your NATed networks.

Adding a NATed Network to QRadar Log Manager

Using the deployment editor, you can add NATed network to your deployment.

Before you begin

Before you enable NAT for a managed host, you must set up your NATed networks using static NAT translation. This ensures communications between managed hosts that exist within different NATed networks.

Example

The QFlow 1101 in Network 1 has an internal IP address of 10.100.100.1. When the QFlow 1101 wants to communicate with the Event Collector in Network 2, the NAT router translates the IP address to 192.15.2.1.

Procedure

Step 1 In the deployment editor, click the **NATed Networks** icon.

Step 2 Click **Add**.

Step 3 Type a name for a network you want to use for NAT.

Step 4 Click **OK**.

The Manage NATed Networks window is displayed, including the added NATed network.

Step 5 Click **OK**.

Step 6 Click **Yes**.

Editing a NATed network

Using the deployment editor, you can edit a NATed network.

Procedure

Step 1 In the deployment editor, click the **NATed Networks** icon.

Step 2 Select the NATed network you want to edit. Click **Edit.**

Step 3 Type a new name for of the NATed network.

Step 4 Click **OK**.

The Manage NATed Networks window is displayed, including the updated NATed networks.

Step 5 Click **OK**.

Step 6 Click **Yes**.

Deleting a NATed network From QRadar Log Manager

Using the deployment editor, you can delete a NATed network from your deployment:

Procedure

Step 1 In the deployment editor, click the **NATed Networks** icon.

Step 2 Select the NATed network you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Step 5 Click **Yes**.

Changing the NAT status for a Managed Host

Using the deployment editor, you can 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 NATed 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 Log Manager before you update the device. This prevents the host from becoming unreachable and allows you to deploy changes to that host.

About this task

When you change the NAT status for an existing managed host, error messages might be displayed. Ignore these error messages.

Procedure

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Right-click the managed host you want to edit and select **Edit Managed Host**.

Step 3 Click **Next**.

Step 4 Choose one of the following options:

a If you want to enable NAT for the managed host, select the **Host is NATed** check box and click **Next**. Go to **Step 5**.

b If you want to disable NAT for the managed host, clear the **Host is NATed** check box. Go to **Step 6**.

Step 5 To select a NATed network, enter values for the following parameters:

- **Change public IP of the server or appliance to add** - Type the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.
- **Select NATed network** - From the list box, select the network you want this managed host to use.

- **Manage NATs List** - Click this icon to update the NATed network configuration. For more information, see **NAT management**.

Step 6 Click **Next**.

Step 7 Click **Finish**.

Step 8 Update the configuration for the device (firewall) to which the managed host is communicating.

Step 9 On the **Admin** tab menu, select **Advanced > Deploy Full Configuration**.

Component configuration

Using the deployment editor, you can configure each component in your deployment.

Configuring an Event Collector

Use the deployment editor to configure an Event Collector.

About this task

For an overview of the Event Collector component, see **QRadar Log Manager components**.

The following table describes the advanced Event Collector parameters:

Table 8-6 Event Collector advanced parameters

Parameter	Description
Primary Collector	Specifies one of the following values: • **True** - Specifies that the Event Collector is located on a Console system. • **False** - Specifies that the Event Collector is located on a non-Console system.
Autodetection Enabled	Type of the following values: • **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 is the default. • **No** - Prevents the Event Collector from automatically analyzing and accepting traffic from previously unknown log sources. For more information on configuring log sources, see the *Managing Log Sources Guide.*
Forward Events Already Seen	Type one of the following options: • **True** - Enables the Event Collector to forward events that have already been detected on the system. • **False** - Prevents the Event Collector from forwarding events that have already been detected on the system. This prevents event looping on your system.

Procedure

Step 1 From either the Event View or System View pages, select the Event Collector you want to configure.

Step 2 From the menu, select **Actions > Configure**.

Step 3 Enter values for the following parameters:

Parameter	Description
Destination Event Processor	Specifies the Event Processor component connected to this QFlow Collector. The connection is displayed in the following format: <Host IP Address>:<Port>. If the QFlow Collector is not connected to an Event Processor, the parameter is empty.
Event Forwarding Listen Port	Type the Event Collector event forwarding port.

Step 4 On the toolbar, click **Advanced** to display the advanced parameters. See **Table 8-6**.

Step 5 Configure the advanced parameters, as required.

Step 6 Click **Save**.

Step 7 Repeat for all Event Collectors in your deployment you want to configure.

Configuring an Event Processor

Use the deployment editor to configure an Event Processor.

About this task

For an overview of the Event Processor component, see **QRadar Log Manager components**.

The following table describes the advanced Event Processor parameters:

Table 8-7 Event Processor advanced parameters

Parameter	Description
Test Rules	***Note:*** *The* ***test rules*** *list box is available for non-Console Event Processors only. If a rule is configured to test locally, the Globally option does not override the rule setting.* Type one of the following options: • **Locally** - Rules are tested on the Event Processor and not shared with the system. • **Globally** - Allows individual rules for every Event Processor to be shared and tested system wide. Each rule in **Log Activity > Rules** 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 is five failed login attempts within 5 minutes. When the Event Processor containing the local rule observes five failed login attempts, the rule generates a response. When the rule in the example above is set to Global, when five failed login attempts within 5 minutes is 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 Processors, with each rule on the Event Processor set 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.
Events database path	Type the location you want to store events. The default is **`/store/ariel/events`**.
Payloads database length	Type the location you want to store payload information. The default is **`/store/ariel/payloads`**.

Procedure

Step 1 From either the Event View or System View pages, select the Event Processor you want to configure.

Step 2 From the menu, select **Actions > Configure**.

Step 3 Enter values for the parameters:

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

Step 4 On the toolbar, click **Advanced** to display the advanced parameters.

Step 5 Enter values for the parameters, as necessary. See **Table 8-7**.

Step 6 Click **Save**.

Step 7 Repeat for all Event Processors in your deployment you want to configure.

Configuring the Magistrate

Use the deployment editor to configure a Magistrate component.

About this task

For an overview of the Magistrate component, see **QRadar Log Manager components**.

Procedure

Step 1 From either the Event View or System View pages, select the Magistrate component you want to configure.

Step 2 From the menu, select **Actions > Configure**.

Step 3 On the toolbar, click **Advanced** to display the advanced parameters.

Step 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.

Step 5 Click **Save**.

Configuring an off-site source

Use the deployment editor to configure a off-site source.

About this task

For an overview of the off-site source component, see **QRadar Log Manager components**.

When configuring off-site source and target components, deploy the Console with the off-site source first and the Console with the off-site target second to prevent connection errors.

Procedure

Step 1 From either the Event View or System View pages, select the off-site source you want to configure.

Step 2 From the menu, select **Actions > Configure**.

Step 3 Enter values for the parameters:

Parameter	Description
Receive Events	Type one of the following values: • **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.

Step 4 Click **Save**.

Step 5 Repeat for all off-site sources in your deployment you want to configure.

Configuring an off-site target

Use the deployment editor to configure a off-site target.

About this task

For an overview of the off-site target component, see **QRadar Log Manager components**.

When configuring off-site source and target components, we recommend that you deploy the Console with the off-site source first and the Console with the off-site target second to prevent connection errors.

Procedure

Step 1 From either the Event View or System View pages, select the off-site target you want to configure.

Step 2 From the menu, select **Actions > Configure**.

Step 3 Enter values for the parameters:

Parameter	Description
Event Collector Listen Port	Type the Event Collector listen port for receiving event data. The default listen port for events is 32004. ***Note:*** *If the off-site target system has been upgraded from a previous QRadar Log Manager software version, you must change the port from the default (32004) to the port specified in the* ***Event Forwarding Listen Port*** *parameter for the off-site target. For more information on how to access the Event Forwarding Listen port on the off-site target, see* **Configuring an Event Collector***.*

Step 4 Click **Save**.

9 FORWARDING EVENT DATA

You can configure IBM Security QRadar Log Manager to forward event data to one or more vendor systems, such as ticketing or alerting systems.

Event forwarding overview

QRadar Log Manager allows you to forward raw log data received from log sources to one or more vendor systems, such as ticketing or alerting systems. You can also forward QRadar Log Manager-normalized event data to other QRadar Log Manager systems. On the QRadar Log Manager user interface, these vendor systems are called forwarding destinations. QRadar Log Manager ensures that all forwarded data is unaltered.

To configure QRadar Log Manager to forward events, you must first configure one or more forwarding destinations. Then you can configure routing rules, custom rules, or both to determine what log data you want to forward and what routing options apply to the log data.

For example, you can configure all log data from a specific event collector to forward to a specific vendor ticketing system. You can also choose from various routing options such as removing the log data that matches a routing rule from your QRadar Log Manager system and bypassing correlation. Correlation is the process of matching events to rules, which in turn can generate events.

Add forwarding destinations

Before you can configure bulk or select event forwarding, you must add forwarding destinations on the Forwarding Destinations window.

About this task

The following table describes the Forwarding Destinations parameters:

Table 9-1 Forwarding Destinations parameters

Parameter	Description
Name	Type a unique name for the forwarding destination.
Event Format	From the list box, select an event format. Options include: • **Raw event** - Raw event data is event data in the format that the log source sent. This is the default option. • **Normalized event** - Normalized data is raw event data that QRadar Log Manager has parsed and prepared for the display as readable information on the QRadar Log Manager user interface. ***Note:*** *Normalized event data cannot transmit using the UDP protocol. If you select the* ***Normalized Event*** *option, the* ***UDP*** *option in the* ***Protocol*** *list box is disabled.*
Destination Address	Type the IP address or host name of the vendor system you want to forward event data to.
Destination Port	Type the port number of the port on the vendor system you want to forward event data to. The default port is 514.
Protocol	Using the list box, select the protocol you want to use to forward event data. Choices include: • **TCP** - Transmission Control Protocol. To send normalized event data using the TCP protocol, you must create an off-site source at the destination address on port 32004. For more information on creating off-site sources, see **Using the deployment editor**. • **UDP** - User Datagram Protocol Normalized event data cannot transmit using the UDP protocol. If you select the UDP option, the **Normalized Event** option in the **Event Format** list box is disabled. The default protocol is TCP.

Table 9-1 Forwarding Destinations parameters (continued)

Parameter	Description
Prefix a syslog header if it is missing or invalid	When QRadar Log Manager forwards syslog messages, the outbound message is verified to ensure it has a proper syslog header. ▶ Select this check box to prefix a syslog header if a header is not detected on the original syslog message. The prefixed syslog header includes the QRadar Log Manager appliance host name in the **Hostname** field of the syslog header. If this check box is clear, the syslog message is sent unmodified.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 On the toolbar, click **Add**.

Step 5 On the Forwarding Destinations window, enter values for the parameters. See Table 9-1.

Step 6 Click **Save**.

Result

The forwarding destination you added is now displayed on the Forwarding Destinations window. The forwarding destination is enabled by default and is available for you to include in routing rules and custom rules. For more information on managing forwarding destinations, see **Forwarding destinations management tasks**.

Configuring bulk event forwarding

After you have added one or more forwarding destinations, you can create filter-based routing rules to allow QRadar Log Manager to forward large quantities of event data.

About this task

The following table describes the Event Routing Rules window parameters:

Table 9-2 Event Routing Rules parameters

Parameter	Description
Name	Type a unique name for the routing rule.
Description	Type a description for the routing rule.

Table 9-2 Event Routing Rules parameters (continued)

Parameter	Description
Forwarding Event Collector	From the list box, select the event collector you want to forward events from.
Current Filters	
Match All Incoming Events	Select this check box to specify that you want this rule to forward all incoming events. If you select this option, the **Add Filter** functionality is no longer displayed.
Add Filter	Using the options in the Current Filters pane, configure your filters: **1** From the first list box, select a property you want to filter for. Options include all normalized and custom event properties. **2** From the second list box, select an operator. Choices include **Equals** and **Equals any of**. **3** In the text box, type the value you want to filter for. **4** Click **Add Filter**. **5** Repeat for each filter you want to add.
Routing Options	
Forward	Select this check box to forward log data that matches the current filters, and then select the check box for each forwarding destination that forward log data to. 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. For more information, see **Forwarding destinations management tasks**.
Drop	Select this check box if you to remove the log data that matches the current filters from the QRadar Log Manager database. ***Note:*** *If you select the* ***Drop*** *check box, the* ***Bypass Correlation*** *check box is automatically cleared.*
Bypass Correlation	Select this check box if you want the log data that matches the current filters to bypass correlation. When correlation is bypassed, the log data that matches the current filter is stored in the QRadar Log Manager database, but it is not tested in the CRE. ***Note:*** *If you select the* ***Bypass Correlation*** *check box, the* ***Drop*** *check box is automatically cleared.*

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Routing Rules** icon.

Step 4 On the toolbar, click **Add**.

Step 5 On the Event Routing Rules window, enter values for the parameters. See **Table 9-2**.

Step 6 Click **Save**.

Result

The routing rule is now displayed on the Event Routing Rules window. The routing rule is enabled by default and automatically starts processing events for bulk forwarding. For more information on managing routing rules, see **Managing routing rules**.

Configuring selective event forwarding

Using the Custom Rule Wizard, you can configure rules to forward event data to one or more forwarding destinations as a rule response. This task provides you a means to configure highly selective event forwarding.

About this task

The criteria for what data gets forwarded to a forwarding destination is based on the tests and building blocks included in the rule. When the rule is configured and enabled, all events matching the rule tests are automatically forwarded to the specified forwarding destinations. For more information on how to edit or add a rule, see the *IBM Security QRadar Log Manager Users Guide*.

Procedure

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

Step 2 Select **Rules**.

Step 3 Edit or add a rule, ensuring that you select the **Send to Forwarding Destinations** option on the Rule Response page in the Rule Wizard.

Forwarding destinations management tasks

Use the Forwarding Destination window to view, edit, and delete forwarding destinations.

Viewing forwarding Destinations

The Forwarding Destinations window provides valuable information on your forwarding destinations, including statistics for the data sent to each forwarding destination.

About this task

The Forwarding Destinations window provides the following information:

Table 9-3 Forwarding Destination window parameters

Parameter	Description
Name	Specifies the name of this forwarding destination.
Event Format	Specifies whether raw event data or normalized event data is sent to this forwarding destination.
Host / IP Address	Specifies the IP address or host name of this forwarding destination host.
Port	Specifies the receiving port on this forwarding destination host.
Protocol	Specifies whether the protocol for this forwarding event data is TCP or UDP.
Seen	Specifies how many total number events were seen for this forwarding destination.
Sent	Specifies how many events have actually been sent to this forwarding destination.
Dropped	Specifies how many events have been dropped before reaching this forwarding destination.
Enabled	Specifies whether this forwarding destination is enabled or disabled. For more information, see **Enabling and disabling a forwarding destination**.
Creation Date	Specifies the date that this forwarding destination was created.
Modification Date	Specifies the date that this forwarding destination was last modified.

The Forwarding Destinations window toolbar provides the following functions:

Table 9-4 Forwarding Destinations window toolbar

Function	Description
Add	Click **Add** to add a new forwarding destination. See **Add forwarding destinations**.
Edit	Click **Edit** to edit a selected forwarding destination. See **Editing a forwarding destination**.
Enable/Disable	Click **Enable/Disable** to enable or disable a selected forwarding destination. For more information, see **Enabling and disabling a forwarding destination**.
Delete	Click **Delete** to delete a selected forwarding destination. See **Delete a forwarding destination**.
Reset Counters	Click **Reset Counters** to reset the **Seen**, **Sent**, and **Dropped** parameters for all forwarding destinations back to zero (0). See **Resetting the counters**.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 View the statistics for your forwarding destinations. See **Table 9-3**.

Enabling and disabling a forwarding destination

When you create a forwarding destination, it is enabled by default. Using the **Enable/Disable** icon, you can toggle the forwarding destination on or off.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to enable or disable.

Step 5 On the toolbar, click **Enable/Disable**.

Resetting the counters

The **Seen**, **Sent**, and **Dropped** parameters provide counts that continue to accumulate until you reset the counters. You can reset the counters to provide a more targeted view of how your forwarding destinations are performing.

About this task

After you reset the counters, the **Seen**, **Sent**, and **Dropped** parameters display a value of zero (0), until the counters start accumulating again.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 On the toolbar, click **Reset Counters**.

Editing a forwarding destination

You can edit a forwarding destination to change the configured name, format, IP address, port, or protocol.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters, as necessary. See **Table 9-1**.

Step 7 Click **Save**.

Delete a forwarding destination

You can delete a forwarding destination. If the forwarding destination is associated with any active rules, you must confirm that you want to delete the forwarding destination.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Forwarding Destinations** icon.

Step 4 Select the forwarding destination you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

Managing routing rules

Use the Event Routing Rules window to view, edit, enable, disable, or delete a rule.

Viewing rules

The Event Routing Rules window provides valuable information on your routing rules, such as the configured filters and actions that are performed when event data matches each rule.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Routing Rules** icon.

Editing a routing rule

You can edit a routing rule to change the configured name, Event Collector, filters, or routing options.

About this task

The Event Routing Rules window provides the following information:

Table 9-5 Event Routing Rules window parameters

Parameter	Description
Name	Specifies the name of this routing rule.
Event Collector	Specifies the Event Collector you want this routing rule process data from.
Filters	Specifies the configured filters for this routing rule.

Table 9-5 Event Routing Rules window parameters (continued)

Parameter	Description
Routing Options	Specifies the configured routing options for this routing rule. Options include: • **Forward** - Event data is forwarded to the specified forwarding destination. Event data is also stored in the database and processed by the Custom Rules Engine (CRE). • **Forward & Drop** - Event data is forwarded to the specified forwarding destination. Event data is not stored in the database and is processed by the CRE. • **Forward & Bypass** - Event data is forwarded to the specified forwarding destination. Event data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the event. • **Drop** - Event data is not stored in the database and is not processed by the CRE. The event data is not forwarded to a forwarding destination, but it is processed by the CRE. • **Bypass** - Event data is not processed by the CRE, but it is stored in the database. If an event matches multiple rules, the safest routing option is applied. For example, if an event that matches a rule configured to drop the event and a rule to bypass CRE processing, the event is not dropped. Instead, the event bypasses the CRE and is stored in the database. All events, regardless of the routing option, is counted against the EPS license.
Enabled	Specifies whether this routing rule is enabled or disabled.
Creation Date	Specifies the date that this routing rule was created.
Modification Date	Specifies the date that this routing rule was modified.

The Event Routing Rules window toolbar provides the following functions:

Table 9-6 Event Routing Rules window toolbar

Function	Description
Add	Click **Add** to add a new routing rule. See **Configuring bulk event forwarding**.
Edit	Click **Edit** to edit a selected routing rule. See **Editing a routing rule**.
Enable/Disable	Click **Enable/Disable** to enable or disable a selected routing rule. See **Enabling or disabling a routing rule**.

Table 9-6 Event Routing Rules window toolbar (continued)

Function	Description
Delete	Click **Delete** to delete a selected routing rule. For more information, see **Deleting a routing rule**.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Routing Rules** icon.

Step 4 Select the routing rule you want to edit.

Step 5 On the toolbar, click **Edit**.

Step 6 Update the parameters, as necessary. See **Table 9-5**.

Step 7 Click **Save**.

Enabling or disabling a routing rule

When you first create a routing rule, it is enabled by default. Using the **Enable/Disable** icon, you can toggle the routing rule on or off. To enable or disable a routing rule:

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Routing Rules** icon.

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

Step 5 On the toolbar, click **Enable/Disable**.

Step 6 If enabled a routing rule that is configured to drop events, a confirmation message is displayed. Click **OK**.

Deleting a routing rule

You can delete a routing rule. You are required to confirm that you want to delete the routing rule.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Routing Rules** icon.

Step 4 Select the routing rule you want to delete.

Step 5 On the toolbar, click **Delete**.

Step 6 Click **OK**.

10 STORING AND FORWARDING EVENTS

Store and Forward allows you to manage schedules that control when to start and stop forwarding events from your dedicated Event Collector appliances to Event Processors in your deployment.

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 *IBM Security 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

The Store and Forward window provides a list of schedules that includes statistics to help you evaluate the status, performance, and progress of your schedules.

Before you begin

By default, no schedules are listed the first time you access the Store and Forward window. For more information on adding a schedule, see **Creating a New Store and Forward Schedule**.

About this task

You can use options on the toolbar and the **Display** list box to change your view of the schedule list. Changing your view of the list allows you 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

box. The list then groups by the **Event Collector** column and makes it easier for you to locate the Event Collector you want to investigate.

By default, the Store and Forward list is configured to display the list organized by the schedule (**Display > Schedules**) and provides the following information:

Table 10-1 Store and Forward window parameters

Parameter	Description
Display	From the **Display** list box, select one of the following options: • **Schedules** - When you select **Schedules** from the **Display** list box, the list displays a hierarchy tree that shows the parent-child relationship between the Schedules, Event Processors, and the associated Event Collectors. • **Event Collectors** - When you select **Event Collectors** from the **Display** list box, the list displays the lowest level in the hierarchy, which is a list of Event Collectors. Therefore, the list does not display a hierarchy tree. • **Event Processors** - When you select **Event Processors** from the **Display** list box, the list displays a hierarchy tree that shows the parent-child relationship between the Event Processors and the associated Event Collectors.
Name	Displays the name of the schedule, Event Collector, or Event Processor, depending on the level of the hierarchy tree. When you select **Schedules** from the **Display** list box, the values in the **Name** column are displayed as follows. • **First Level** - Displays the name of the schedule. • **Second Level** - Displays the name of the Event Processor. • **Third Level** - Displays the name of the Event Collector. When you select **Event Processors** from the **Display** list box, the values in the **Name** column are displayed as follows: • **First Level** - Displays the name of the Event Processor. • **Second Level** - Displays the name of the Event Collector. ***Note:*** *This parameter is displayed only when you select **Schedules** or **Event Processors** from the **Display** list box.* 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 using options on the toolbar. See **Table 10-2**.
Schedule Name	Displays the name of the schedule. ***Note:*** *This parameter is displayed only when you select **Event Collectors** or **Event Processors** from the **Display** list box.* If an Event Processor is associated with more than one schedule, the **Schedule Name** parameter displays the following text: `Multiple(n)`, where n is the number of schedules. You can click the plus symbol (+) to view the associated schedules.

Table 10-1 Store and Forward window parameters (continued)

Parameter	Description
Event Collector	Displays the name of the Event Collector. ***Note:** This parameter is displayed only when you select **Event Collectors** from the **Display** list box.*
Event Processor	Displays the name of the Event Processor. ***Note:** This parameter is displayed only when you select **Event Collectors** or **Event Processors** from the **Display** list box.*
Last Status	Displays the status of the Store and Forward process. Statuses include: • **Forwarding** - Indicates that event forwarding is in progress. • **Forward Complete** - Indicates that event forwarding has successfully completed and events are currently being stored locally on the Event Collector. The stored events will be forwarded when the schedule indicates that forwarding can start again. • **Warn** - Indicates that the percentage of events remaining in storage exceeds the percentage of time remaining in the Store and Forward schedule. • **Error** - Indicates that event forwarding ceased before all stored events were forwarded. • **Inactive** - Indicates that this schedule is inactive, because no Event Collectors are assigned to it or the assigned Event Collectors are not receiving any events. You can move your mouse pointer over the **Last Status** column to view a summary of the status. The summary includes the following information: • **Total Events to be Transferred** - Displays the total number of events that were stored during the period of time between the configured **Forward End** and the **Forward Start** times. • **Number of Events Transferred** - Displays the number of events successfully forwarded. • **Events Remaining** - Displays the number of events remaining to be transferred. • **Percentage Transferred** - Displays the percentage of events successfully forwarded.
	• **Forward Start** - Displays the actual time that forwarding started. The time is displayed in the following format: `yyyy-mm-dd hh:mm:ss`. • **Forward Last Update** - Displays the time when the status was last updated. The time is displayed in the following format: `yyyy-mm-dd hh:mm:ss`. • **Forwarding Time Remaining** - Displays the amount of time remaining in the Store and Forward schedule.

Table 10-1 Store and Forward window parameters (continued)

Parameter	Description
Percent Complete	Displays the percentage of events forwarded during the current session.
Forwarded Events	Displays the number of events (in K, M, or G) forwarded in the current session. You can move your mouse pointer over the value in the **Forwarded Events** column to view the actual number of events.
Remaining Events	Displays the number of events (in K, M, or G) remaining to be forwarded in the current session. You can move your mouse pointer over the value in the **Remaining Events** column to view the actual number of events.
Time Elapsed	Displays the amount of time that has elapsed since the current forwarding session started.
Time Remaining	Displays the amount of time remaining in the current forwarding session.
Average Event Rate	Displays the average Event Per Second (EPS) rate during this session. The EPS rate is the rate at which events are forwarding from the Event Collector to the Event Processor. You can move your mouse pointer over the value in the **Average Event Rate** column to view the actual average EPS.
Current Event Rate	Displays the current Event Per Second (EPS) rate during this session. The EPS rate is the rate at which events are forwarding from the Event Collector to the Event Processor. You can move your mouse pointer over the value in the **Current Event Rate** column to view the actual current EPS.
Forward Schedule	Displays the time at which events are scheduled to start forwarding.
Transfer Rate Limit	Displays the rate at which events are forwarding. The transfer rate limit is configurable. The transfer rate limit can be configured to display in Kilobits per second (Kps), Megabits per second (Mps), or Gigabits per second (Gps). To edit the transfer rate limit, see **Editing a Store and Forward Schedule**.
Owner	Displays the user name that created this schedule.
Creation Date	Displays the date when this schedule was created.
Last Modified	Displays the date when this schedule was last edited.

The toolbar provides the following options:

Table 10-2 Store and Forward - Schedules Window Parameters

Option	Description
Actions	Click **Actions** to perform the following actions: • **Create** - Click this option to create a new schedule. See **Creating a New Store and Forward Schedule**. • **Edit** - Click this option to edit an existing schedule. See **Editing a Store and Forward Schedule**. • **Delete** - Click this option to delete a schedule. See **Deleting a Store and Forward Schedule**.
Expand All	Click **Expand All** to expand the list to display all levels in the hierarchy tree, including the schedule, Event Processor, and Event Collector levels.
Collapse All	Click **Collapse All** to display only the first level of the hierarchy tree.
Search Schedules	Type your search criteria in the **Search Schedules** field and click the **Search Schedules** icon or press Enter on your keyboard. The list updates to display search results based on which option is selected in the **Display** list box: • **Schedules** - When you select **Schedules** from the **Display** list box, schedules that match your search criteria are displayed in the list. • **Event Collectors** - When you select **Event Collectors** from the **Display** list box, Event Collectors that match your search criteria are displayed in the list. • **Event Processors** - When you select **Event Processors** from the **Display** list box, Event Processors that match your search criteria are displayed in the list.
Last Refresh	Indicates the amount of time that has elapsed since this window was refreshed.
Pause	Click the **Pause** icon to pause the timer on the Store and Forward window. Click the **Play** icon to restart the timer.
Refresh	Click the **Refresh** icon to refresh the Store and Forward window.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Store and Forward** icon.

Step 4 On the Store and Forward window, view the parameters for each schedule.

Creating a New Store and Forward Schedule

The Store and Forward Schedule Wizard allows you to create a schedule that controls when your Event Collector starts and stops forwarding data to an Event Processor for event processing.

Before you begin

The connection between an Event Collector and an Event Processor is configured in the Deployment Editor. Before you can create a new schedule, you must ensure that your dedicated Event Collector is added to your deployment and connected to an Event Processor. For more information on adding and connecting an Event Processor to your deployment, see **Event view management**.

About this task

You can create and manage multiple schedules to control event forwarding from multiple Event Collectors in a geographically distributed deployment.

The following table describes the Select Collectors page parameters:

Table 10-3 Store and Forward Schedule Wizard - Select Collectors Page Parameters

Parameter	Description
Schedule Name	Type a unique name for the schedule. You can type a maximum of 255 characters.
Available Event Collectors	Select one or more Event Collectors from the **Available Event Collectors** list and click the Add Event Collector (>) icon. When you add an Event Collector, the Event Collector is displayed in the **Selected Event Collectors** list. ***Note:*** *You can filter the* ***Available Event Collectors*** *list by typing a keyword in the* ***Type to filter*** *field.* If the Event Collector you want to configure is not listed, the Event Collector might not have been added to your deployment. If this occurs, you need to access the Deployment Editor to add the Event Collector before you proceed. See **Using the deployment editor**.

Table 10-3 Store and Forward Schedule Wizard - Select Collectors Page Parameters

Parameter	Description
Selected Event Collectors	Displays a list of selected Event Collectors. You can remove Event Collectors from this list. To remove an Event Collector from the **Selected Event Collectors** list: ▶ Select the Event Collector from the **Selected Event Collectors** list and click the Remove Event Collector (<) icon. ***Note:*** *You can filter the* ***Selected Event Collectors*** *list by typing a keyword in the* ***Type to filter*** *field.* When you remove an Event Collector from the **Selected Event Collectors** list, the removed Event Collector is displayed in the **Available Event Collectors** list.

The following table describes the Schedule Options page parameters:

Table 10-4 Store and Forward Schedule Wizard - Schedule Options Page Parameters

Parameter	Description
Forward Transfer Rate (0 for unlimited)	Configure the forward transfer rate you want this schedule to use when forwarding events from the Event Collector to the Event Processor. To configure the forward transfer rate: **1** From the first list box, type or select a number. 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. **2** From the second list box, select a unit of measurement. Options include: Kilobits per second, Megabits per second, and Gigabits per second.
Scheduling Information	Select this check box to display the following scheduling options: • Forward Time Zone • Forward Start • Forward End
Forward Time Zone	From this list box, select your time zone. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.*

Table 10-4 Store and Forward Schedule Wizard - Schedule Options Page Parameters

Parameter	Description
Forward Start	Configure what time you want event forwarding to start: **1** From the first list box, select the hour of the day when you want to start forwarding events. **2** From the second list box, select AM or PM. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.* ***Note:*** *If the* ***Forward Start*** *and* ***Forward End*** *parameters specify the same time, events are always forwarded. For example, if you configure a schedule to forward events from 1 AM to 1 AM, event forwarding does not cease.*
Forward End	Configure what time you want event forwarding to end: **1** From the first list box, select the hour of the day when you want to stop forwarding events. **2** From the second list box, select AM or PM. ***Note:*** *This option is only displayed when the Scheduling Information check box is selected.* ***Note:*** *If the* ***Forward Start*** *and* ***Forward End*** *parameters specify the same time, events are always forwarded. For example, if you configure a schedule to forward events from 1 AM to 1 AM, event forwarding does not cease.*

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Store and Forward** icon.

Step 4 From the **Actions** menu, select **Create**.

Step 5 Click **Next** to move to the Select Collectors page.

Step 6 On the Select Collectors page, configure the parameters. See **Table 10-3**.

Step 7 Click **Next** to move to the Schedule Options page.

Step 8 On the Schedule Options page, configure the parameters. See **Table 10-4**.

Step 9 Click **Next** to move to the Summary page.

Step 10 On the Summary page, confirm the options you configured for this Store and Forward schedule.

Step 11 Click **Finish**.

Result

Your Store and Forward schedule is saved and 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. For more information on viewing the Store and Forward window, see **Viewing the Store and Forward Schedule list**.

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 schedule's statistics displayed in the Store and Forward list are reset.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Store and Forward** icon.

Step 4 Select the schedule you want to edit.

Step 5 From the **Actions** menu, select **Edit**.

Note: You can also double-click a schedule for editing.

Step 6 Click **Next** to move to the Select Collectors page.

Step 7 On the Select Collectors page, edit the parameters. For more information on the Select Collectors page parameters, see **Table 10-3**.

Step 8 Click **Next** to move to the Schedule Options page.

Step 9 On the Schedule Options page, edit the scheduling parameters. For more information on the Schedule Options page parameters, see **Table 10-4**.

Step 10 Click **Next** to move to the Summary page.

Step 11 On the Summary page, confirm the options you edited for this schedule.

Step 12 Click **Finish**.

Result

The Store and Forward Schedule Wizard closes. Your edited schedule is saved and you can now view the updated schedule in the Store and Forward window. After you edit a schedule, it might take up to 10 minutes for statistics to update in the Store and Forward window. For more information on the Store and Forward window, see **Viewing the Store and Forward Schedule list**.

Deleting a Store and Forward Schedule

You can delete a Store and Forward schedule. After you delete a schedule, the associated Event Collectors continuously forward events to the Event Processor.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Store and Forward** icon.

Step 4 Select the schedule you want to delete.

Step 5 From the **Actions** menu, select **Delete**.

Result

The deleted schedule is removed from the Store and Forward window. After the schedule is deleted, the associated Event Collectors resume continuous forwarding of events to their assigned Event Processor.

11 DATA OBFUSCATION

Data obfuscation encrypts sensitive event data to prevent unauthorized access to user identifiable information.

Any information from the event payload can be obfuscated. For example, you can configure user names, credit card numbers, or host name fields to contain obfuscated data. Data obfuscation assists with privacy concerns by unauthorized users to meet regulatory commission requirements or to assist with meeting corporate privacy policies.

Data obfuscation overview

When data obfuscation is configured on an IBM Security QRadar Log Manager, the encrypted version of the data is displayed in the columns and parameters on the user interface. To enable or decrypt obfuscated data, you must use the command-line interface (CLI) utility on the QRadar Log Manager Console.

Data obfuscation occurs at the event level in your QRadar Log Manager deployment. As events are provided to the appliances in your deployment, the raw event is processed and normalized. The obfuscation process evaluates the obfuscation expression and ensures that the raw event and normalized event contain the data that is required to complete the obfuscation. The data that is defined in the obfuscation expression is then matched in the event and the data is encrypted before it is written to the disk.

The obfuscated data from the event pipeline is written in the obfuscated format to the Ariel database. Unauthorized users that attempt to query the database directly cannot view sensitive data without the public and private decryption key.

The obfuscation process requires that you create a public and private key for your IBM Security QRadar Log Manager Console. The public key remains on the Console and the private key must be stored in a secure location. The private key contains the decryption key that is required for administrators to view the unobfuscated data.

Data obfuscation encrypts new events as they are received by QRadar Log Manager. Events in the **`/store`** directory prior to enabling data obfuscation will remain in their current state.

Any log source extensions that change the format of the event payload can cause issues with data obfuscation. Any expressions that you configure can take the parsing that is done by the log source extension in to account.

User names and host name data that are part of the QRadar Log Manager asset profile before your upgrade to QRadar Log Manager 7.2 might not display obfuscated data as expected. To obfuscate asset profile data, you can use **Delete Listed** option from the from **Assets** tab, which removes the unobfuscated hosts and user names. You can then run vulnerability scans and wait for the asset data to repopulate. After a few days you can run the Server Discovery tool to repopulate the data for building blocks on your QRadar Log Manager system.

To obfuscate data on a QRadar Log Manager system, use the following utilities:

- **obfuscation_updater.sh** - Use the obfuscation_updater.sh utility to install the public key on your system and configure regular expression (Regex) statements to define what parameters you want obfuscated.
- **obfuscation_expressions.xml** - Use the obfuscation_expressions.xml file to specify regular expression (regex) statements that identify the data you want to obfuscate. Any text within an event that matches the regular expressions that are specified in the obfuscation_expressions.xml is encrypted, both in the event payload and in any normalized fields.
- **obfuscation_decoder.sh** - When you must investigate the unencrypted version of the data, you must use the obfuscation_decoder.sh utility to decrypt the specific encrypted value you want to investigate.

To configure and manage obfuscated data, perform the following tasks:

1. Generate an RSA private/public key pair. See **Generating a private/public key pair**.
2. Configure data obfuscation. See **Configuring data obfuscation**.
3. When required, decrypt data obfuscation. See **Decrypting obfuscated data**.

Generating a private/public key pair

Data obfuscation and decryption requires an RSA private/public key pair. You must create and format a private key, and then generate a public key.

After you install the public key on your QRadar Log Manager Console. The Console ensures that the managed hosts are obfuscating data to match your obfuscation expression patterns.

About this task

A key pair consists of two separate files: a public and private key. Only one public key can be installed for each system. After you install a public key, the key cannot be overwritten.

Use the following options when you generate a private key:

Table 11-1 Generate private key configuration options

Option	Description
[-out filename]	Use this option to define the file name of the RSA private key file.
[numbits]	Use this option to define the size of the private key. The size is measured in bits. The default size is 512.

Use the following options when you format the RSA private key:

Table 11-2 Format private key configuration options

Option	Description
[-topk8]	Use this option to read a traditional format private key and write the private key in PKCS #8 format.
[-inform]	Use this option to define the input format of the private key as Privacy Enhanced Mail (.PEM). For example: **-inform PEM**
[-outform]	Use this option to define the format of the private key output as .PEM. For example: **-outform PEM**
[-in filename]	Use this option to define the private key file name.
[-out filename]	Use this option to define the output file name.
[-nocrypt]	Specifies that the private key uses the unencrypted PrivateKeyInfo format.

Use the following options when you generate the public key:

Table 11-3 Generate public key configuration options

Option	Description
[-in filename]	Defines the input file name.
[-pubout]	Generates a public key.
[-outform DER]	Defines the file type of the public key file as DER Encoded X509 Certificate file (.DER).
[-out filename]	Defines the public key file name.

Procedure

Step 1 Using SSH, log in to your Console as the root user:

User name: **root**

Password: **<password>**

Step 2 To generate an RSA private key, type the following command:

openssl genrsa [-out filename] [numbits]

For example:

```
openssl genrsa -out mykey.pem 512
```

Step 3 To format the private key, type the following command:

```
openssl pkcs8 [-topk8] [-inform PEM] [-outform PEM] [-in
filename] [-out filename] [-nocrypt]
```

For example:

```
openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out
private_key.pem -nocrypt
```

Step 4 To generate the RSA public key, type the following command:

```
openssl rsa [-in filename] [-pubout] [-outform DER] [-out
filename]
```

For example:

```
openssl rsa -in mykey.pem -pubout -outform DER -out
public_key.der
```

In this example, the following keys were generated:

- mykey.pem
- private_key.pem
- public_key.der

Step 5 After the key is generated, delete the mykey.pem file from your system.

Step 6 To install the public key, type the following command:

```
obfuscation_updater.sh [-k filename]
```

Where **[-k filename]** defines the public key file name to install.

For example:

```
obfuscation_updater.sh -k public_key.der
```

What to do next

To avoid unauthorized access to the obfuscated data, remove the private key file from your system and store it in a secure location and create a backup of the private key.

Configuring data obfuscation

Use the obfuscation_updater.sh script to set up and configure data obfuscation. You can run the obfuscation_updater.sh script from any directory on your Console.

Before you begin

Before you can configure data obfuscation, you must create a private/public key pair. See **Generating a private/public key pair**.

About this task

The obfuscation_expressions.xml file defines the regular expressions that are required to obfuscate data. You can add multiple regular expressions to your obfuscation expression file. The obfuscation_expressions.xml file must contain the following attributes:

Table 11-4 obfuscation_expressions.xml expressions

Attributes	Description
<expression name>	Defines a unique name to identify the regular expression.
<regex>	Defines the regular expression that you want to use to extract the data for obfuscation.
<captureGroup>	Defines the capture group that is associated with the regular expression.
<deviceTypeId>	Identifies the Log Source type. This attribute is used to identify the event and extract the data to be obfuscated. You can obtain the value for this attribute from the sensordeviceType database table or from the *IBM Security QRadar Log Manager Log Sources User Guide*. You can configure a value of -1 to disable this attribute.
<deviceId>	Identifies the Log Source. This attribute is used to identify the event and extract the data to be obfuscated. You can obtain the value for this attribute from the sensordevice database table. You can configure a value of -1 to disable this attribute.
<qidId>	Identifies the Event name. This attribute is used to identify the event and extract the data to be obfuscated. You can obtain the value for this attribute from the qidmap database table. You can configure a value of -1 to disable this attribute.
<category>	Identifies the Low Level Category of the Event. This attribute is used to identify the event and extract the data to be obfuscated. You can obtain the value for this attribute from the category Type database table. You can configure a value of -1 to disable this attribute.
<enabled>	Enables (true) or disables (false) the regular expression.

Example 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
```

Example of an obfuscation_expressions.xml file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ObfuscationExpressions>
    <expression name="VMwareUsers">
```

```
        <regex>usrName=(\S+)</regex>
        <captureGroup>1</captureGroup>
        <deviceTypeId>210</deviceTypeId>
        <deviceId>-1</deviceId>
        <qidId>-1</qidId>
        <category>-1</category>
        <enabled>true</enabled>
    </expression>

    <expression name="VMwarehosts">
        <regex>host=(\S+)</regex>
        <captureGroup>1</captureGroup>
        <deviceTypeId>210</deviceTypeId>
        <deviceId>-1</deviceId>
        <qidId>-1</qidId>
        <category>-1</category>
        <enabled>true</enabled>
    </expression>
</ObfuscationExpressions>
```

Table 11-1 Example regex patterns that can parse user names

Example regex patterns	Matches
`usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-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]$`	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
`usrName=(/S+)`	Matches any non-white space after the equals sign. This is a greedy regular expression and can lead to system performance issues.
`msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Matches users with IP address. For example, root@1.1.1.1
`src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Matches IP address formats.
`host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$`	hostname.ibm.com, hostname.co.uk,

Procedure

Step 1 Using SSH, log in to your Console as the root user:

User name: **`root`**

Password: **`<password>`**

Step 2 Configure the attributes in your **`obfuscation_expressions.xml`** file.

For more information, see **Table 11-4**.

Step 3 To configure data obfuscation, type the following command:

`obfuscation_updater.sh [-p filename] [-e filename]`

Where:

- **`[-p filename]`** defines the Private Key input filename.
- **`[-e filename]`** defines the Obfuscation Expression XML input filename.

For example:

`obfuscation_updater.sh -p private_key.pem -e obfuscation_expressions.xml`

Step 4 Verify that the expression is obfuscated in the QRadar Log Manager interface.

Step 5 Optional. Repeat this process to update your QRadar Log Manager Console with any changes to your **`obfuscation_expressions.xml`** file.

Each time a change is made to the expression, the administrator must verify that the change properly obfuscates the data in the QRadar Log Manager interface.

Decrypting obfuscated data

When suspicious activity occurs on your network, you might be required to decrypt obfuscated data to investigate security issues and users that are involved in suspicious activity. Use the obfuscation_decoder.sh script to decrypt obfuscated data.

Before you begin

Before you begin, you must log in to the QRadar Log Manager user interface and copy the obfuscated text that you want to decrypt.

About this task

Use the following obfuscation_decoder.sh options to decrypt obfuscated data:

Table 11-2 Decryption utility parameters

Option	Description
-k publickey filename	Specifies the public key file name.
-p privatekey filename	Specifies the private key file name.
-d obfuscated text	Specifies the obfuscated text that you want to decrypt.

Procedure

Step 1 Using SSH, log in to your Console as the root user:

User name: **`root`**

Password: **`<password>`**

Step 2 Create a directory and copy the public and private key file to the directory.

Step 3 Navigate to the directory where the keys are located.

Step 4 To decrypt the obfuscated text, type the following command.

```
obfuscation_decoder.sh -k publickey filename -p privatekey
filename -d <obfuscated_text>
```

For example:

```
obfuscation_decoder.sh -k public_key.der -p private_key.pem -d
obfuscated_text
```

Result

The decrypted data is displayed.

What to do next

To avoid unauthorized access to the obfuscated data, remove the private key file from your system and store it in a secure location and create a backup of the private key.

A VIEWING AUDIT LOGS

Changes made by IBM Security QRadar Log Manager users are recorded in the audit logs. You can view the audit logs to monitor changes to QRadar Log Manager and the users performing those changes.

Audit log overview

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches a size of 200 MB. The current log file is named **`audit.log`**. When the file reaches a size of 200 MB, the file is compressed and renamed as follows: **`audit.1.gz, audit.2.gz`**, with the file number incrementing each time a log file is archived. QRadar Log Manager stores up to 50 archived log files.

Viewing the audit log file

Use SSH to log in to your QRadar Log Manager system and monitor changes to your system.

About this task

You can also view normalized audit log events using the **Log Activity** tab.

The maximum size of any audit message (not including date, time, and host name) is 1024 characters.

Each entry in the log file displays using the following format:

`<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>`

Where:

`<date_time>` is the date and time of the activity in the format: Month Date HH:MM:SS.

`<host name>` is the host name of the Console where this activity was logged.

`<user>` is the name of the user that performed the action.

`<IP address>` is the IP address of the user that performed the action.

`(thread ID)` is the identifier of the Java™ thread that logged this activity.

`<category>` is the high-level category of this activity.

`<sub-category>` is the low-level category of this activity.

<action> is the activity that occurred.

<payload> is the complete record that has changed, if any. This might include a user record or an event rule.

Procedure

Step 1 Using SSH, log in to QRadar Log Manager as the root user:

- User Name: **root**
- Password: **<password>**

Step 2 Go to the following directory:

/var/log/audit

Step 3 Open and view the audit log file.

Logged actions

QRadar Log Manager logs the following categories of actions in the audit log file:

Table 12-1 Logged actions

Category	Action
Administrator Authentication	• Log in to the Administration Console. • Log out of the Administration Console.
Assets	• Delete an asset. • Delete all assets.
Audit Log Access	Perform a search that includes events with 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.
Chart Configuration	Save event chart configuration.

Table 12-1 Logged actions (continued)

Category	Action
Custom Property Expressions	• Add a custom event property expression. • Edit a custom event property expression. • Delete a custom event property expression.
Event Retention Buckets	• Add a bucket. • Delete a bucket. • Edit a bucket. • Enable or disable a bucket.
Groups	• Add a group. • Delete a group. • Edit a group.
High Availability	• Add an HA host. • Remove an HA host. • Set an HA system offline. • Set an HA system online. • Restore an HA system.
Index Management	• Enable indexing on a property. • Disable indexing on a property.
Installation	Install a .rpm package, such as a DSM update.
Log Sources	• Add a log source. • Edit a log source. • Delete a log source. • Add a log source group. • Edit a log source group. • Delete a log source group. • Edit the DSM parsing order.
License	• Add a license key. • Revert a license. • Delete a license key.

Table 12-1 Logged actions (continued)

Category	Action
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.
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 (if installed)	• 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.

Table 12-1 Logged actions (continued)

Category	Action
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 Log Manager, as root. • Log out of QRadar Log Manager, 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 a new 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	• Shutdown a system. • Restart a system.

Table 12-1 Logged actions (continued)

Category	Action
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.

B EVENT CATEGORIES

This topic provides a reference of high-level and low-level event categories.

High-level event categories

The high-level event categories include:

Table 13-1 High-level event categories

Category	Description
Recon	Events related to scanning and other techniques used to identify network resources, for example, network or host port scans.
DoS	Events 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	Events related to authentication controls, group, or privilege change, for example, log in or log out.
Access	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
Exploit	Events related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
Malware	Events related to viruses, trojans, back door attacks, or other forms of hostile software. This might include a virus, trojan, malicious software, or spyware.
Suspicious Activity	The nature of the threat is unknown but behavior is suspicious including protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known IDS evasion techniques.
System	Events related to system changes, software installation, or status messages.
Policy	Events regarding corporate policy violations or misuse.
Unknown	Events related to unknown activity on your system.
CRE	Events generated from an offense or event rule. For more information on creating custom rules, see the *IBM Security QRadar Log Manager Administration Guide*.
Potential Exploit	Events relate to potential application exploits and buffer overflow attempts.

Table 13-1 High-level event categories (continued)

Category	Description
User Defined	Events related to user-defined objects.
SIM Audit	Events related to user interaction with the Console and administrative functions.
VIS Host Discovery	Events related to the host, ports, or vulnerabilities that the VIS component discovers.
Application	Events related to application activity.
Audit	Events related to audit activity.
Risk	Events related to risk activity in IBM Security QRadar Risk Manager. ***Note:*** *The Risk high-level category is only displayed on the user interface when IBM Security QRadar Risk Manager is installed.*
Risk Manager Audit	Events related to audit activity in IBM Security QRadar Risk Manager.
Control	Events related to your hardware system diagnostics.
Asset Profiler	Events related to asset profiles.

Recon

The Recon category indicates events related to scanning and other techniques used to identify network resources. The associated low-level event categories include:

Table 13-2 Recon categories

Low level event category	Description	Severity level (0 to 10)
Unknown Form of Recon	Indicates an unknown form of reconnaissance.	2
Application Query	Indicates reconnaissance to applications on your system.	3
Host Query	Indicates reconnaissance to a host in your network.	3
Network Sweep	Indicates reconnaissance on your network.	4
Mail Reconnaissance	Indicates reconnaissance on your mail system.	3
Windows Reconnaissance	Indicates reconnaissance for windows.	3
Portmap / RPC Request	Indicates reconnaissance on your portmap or RPC request.	3
Host Port Scan	Indicates a scan occurred on the host ports.	4

Table 13-2 Recon categories (continued)

Low level event category	Description	Severity level (0 to 10)
RPC Dump	Indicates Remote Procedure Call (RPC) information is removed.	3
DNS Reconnaissance	Indicates reconnaissance on the DNS server.	3
Misc Reconnaissance Event	Indicates a miscellaneous reconnaissance event.	2
Web Reconnaissance	Indicates web reconnaissance on your network.	3
Database Reconnaissance	Indicates database reconnaissance on your network.	3
ICMP Reconnaissance	Indicates reconnaissance on ICMP traffic.	3
UDP Reconnaissance	Indicates reconnaissance on UDP traffic.	3
SNMP Reconnaissance	Indicates 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	Indicates reconnaissance on your UNIX® network.	3
FTP Reconnaissance	Indicates FTP reconnaissance.	3

DoS

The DoS category indicates events related to Denial Of Service (DoS) attacks against services or hosts. The associated low-level event categories include:

Table 13-3 DoS categories

Low level event category	Description	Severity level (0 to 10)
Unknown DoS Attack	Indicates an unknown DoS attack.	8
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

Table 13-3 DoS categories (continued)

Low level event category	Description	Severity level (0 to 10)
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
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

Table 13-3 DoS categories (continued)

Low level event category	Description	Severity level (0 to 10)
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
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 a 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 indicates events related to authentication, sessions and access controls to monitor users on the network. The associated low-level event categories include:

Table 13-4 Authentication categories

Low level event category	Description	Severity level (0 to 10)
Unknown Authentication	Indicates unknown authentication.	1
Host Login Succeeded	Indicates a successful host login.	1
Host Login Failed	Indicates the host login has 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
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 an administrative login has been successful.	1
Admin Login Failure	Indicates the administrative login failed.	3
Suspicious Username	Indicates that a user attempted to access the network using an incorrect user name.	4
Login with username/ password defaults successful	Indicates that a user accessed the network using the default user name and password.	4
Login with username/ password defaults failed	Indicates that a user has been unsuccessful accessing the network using the default user name and password.	4
FTP Login Succeeded	Indicates that the FTP login has been successful.	1

Table 13-4 Authentication categories (continued)

Low level event category	Description	Severity level (0 to 10)
FTP Login Failed	Indicates that the FTP login failed.	3
SSH Login Succeeded	Indicates that the SSH login has been successful.	1
SSH Login Failed	Indicates that the SSH login failed.	2
User Right Assigned	Indicates that user access to network resources has been successfully granted.	1
User Right Removed	Indicates that user access to network resources has been successfully removed.	1
Trusted Domain Added	Indicates that a trusted domain has been successfully added to your deployment.	1
Trusted Domain Removed	Indicates that a trusted domain has been removed from your deployment.	1
System Security Access Granted	Indicates that system security access has been successfully granted.	1
System Security Access Removed	Indicates that system security access has been successfully removed.	1
Policy Added	Indicates that a policy has been successfully added.	1
Policy Change	Indicates that a policy has been successfully changed.	1
User Account Added	Indicates that a user account has been 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 has been successful.	1
User Account Removed	Indicates that a user account has been successfully removed.	1
Group Member Added	Indicates that a group member has been successfully added.	1
Group Member Removed	Indicates that a group member has been removed.	1
Group Added	Indicates that a group has been successfully added.	1
Group Changed	Indicates a change to an existing group.	1

Table 13-4 Authentication categories (continued)

Low level event category	Description	Severity level (0 to 10)
Group Removed	Indicates a group has been removed.	1
Computer Account Added	Indicates a computer account has been successfully added.	1
Computer Account Changed	Indicates a change to an existing computer account.	1
Computer Account Removed	Indicates a computer account has been successfully removed.	1
Remote Access Login Succeeded	Indicates that access to the network using a remote login has been successful.	1
Remote Access Login Failed	Indicates that an attempt to access the network using a remote login failed.	3
General Authentication Successful	Indicates that the authentication processes has been successful.	1
General Authentication Failed	Indicates that the authentication process failed.	3
Telnet Login Succeeded	Indicates that the telnet login has been successful.	1
Telnet Login Failed	Indicates that the telnet login failed.	3
Suspicious Password	Indicates that a user attempted to login using a suspicious password.	4
Samba Login Successful	Indicates a user successfully logged in using Samba.	1
Samba Login Failed	Indicates user login failed using Samba.	3
Auth Server Session Opened	Indicates that a communication session with the authentication server has been started.	1
Auth Server Session Closed	Indicates that a communication session with the authentication server has been closed.	1
Firewall Session Closed	Indicates that a firewall session has been 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 has been successful.	1
Web Service Logout	Indicates that the process to log out of the web service has been successful.	1

Table 13-4 Authentication categories (continued)

Low level event category	Description	Severity level (0 to 10)
Admin Logout	Indicates that the administrative user successfully logged out.	1
FTP Logout	Indicates that the process to log out of the FTP service has been successful.	1
SSH Logout	Indicates that the process to log out of the SSH session has been successful.	1
Remote Access Logout	Indicates that the process to log out using remote access has been successful.	1
Telnet Logout	Indicates that the process to log out of the Telnet session has been successful.	1
Samba Logout	Indicates that the process to log out of Samba has been successful.	1
SSH Session Started	Indicates that the SSH login session has been 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 has been 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 has been detected.	3
IKE Authentication Succeeded	Indicates a successful IKE authentication has been detected.	1
IKE Session Started	Indicates an IKE session started.	1

Table 13-4 Authentication categories (continued)

Low level event category	Description	Severity level (0 to 10)
IKE Session Ended	Indicates an IKE session ended.	1
IKE Error	Indicates an IKE error message.	1
IKE Status	Indicates IKE status message.	1
RADIUS Session Started	Indicates a RADIUS session started.	1
RADIUS Session Ended	Indicates a RADIUS session ended.	1
RADIUS Session Denied	Indicates a RADIUS session has been 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 a TACACS session has been 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 has been successful.	1
Deauthenticating Host Failed	Indicates that the deauthentication of a host failed.	3
Station Authentication Succeeded	Indicates that the station authentication has been successful.	1
Station Authentication Failed	Indicates that the station authentication of a host failed.	3
Station Association Succeeded	Indicates that the station association has been successful.	1
Station Association Failed	Indicates that the station association failed.	3
Station Reassociation Succeeded	Indicates that the station reassociation has been successful.	1
Station Reassociation Failed	Indicates that the station association failed.	3

Table 13-4 Authentication categories (continued)

Low level event category	Description	Severity level (0 to 10)
Disassociating Host Succeeded	Indicates that the disassociating a host has been 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 indicates authentication and access controls for monitoring network events. The associated low-level event categories include:

Table 13-5 Access categories

Low level event category	Description	Severity level (0 to 10)
Unknown Network Communication Event	Indicates an unknown network communication event.	3
Firewall Permit	Indicates access to the firewall has been permitted.	0

Table 13-5 Access categories (continued)

Low level event category	Description	Severity level (0 to 10)
Firewall Deny	Indicates access to the firewall has been 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 the firewall session has been opened.	0
Firewall Session Closed	Indicates the firewall session has been closed.	0
Dynamic Address Translation Successful	Indicates that dynamic address translation has been successful.	0
No Translation Group Found	Indicates that no translation group has been found.	2
Misc Authorization	Indicates that access has been granted to a miscellaneous authentication server.	2
ACL Permit	Indicates that an Access Control List (ACL) permitted access.	0
ACL Deny	Indicates that an Access Control List (ACL) denied access.	4
Access Permitted	Indicates that access has been permitted.	0
Access Denied	Indicates that access has been denied.	4
Session Opened	Indicates that a session has been opened.	1
Session Closed	Indicates that a session has been closed.	1
Session Reset	Indicates that a session has been reset.	3
Session Terminated	Indicates that a session has been terminated.	4
Session Denied	Indicates that a session has been denied.	5
Session in Progress	Indicates that a session is currently in progress.	1
Session Delayed	Indicates that a session has been delayed.	3

Table 13-5 Access categories (continued)

Low level event category	Description	Severity level (0 to 10)
Session Queued	Indicates that a session has been 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 has been detected.	6
Misc Application Action Allowed	Indicates that an application action has been permitted.	1
Misc Application Action Denied	Indicates that an application action has been denied.	3
Database Action Allowed	Indicates that a database action has been permitted.	1
Database Action Denied	Indicates that a database action has been denied.	3
FTP Action Allowed	Indicates that a FTP action has been permitted.	1
FTP Action Denied	Indicates that a FTP action has been denied.	3
Object Cached	Indicates an object cached.	1
Object Not Cached	Indicates an object not cached.	1
Rate Limiting	Indicates that the network is rate limiting traffic.	4
No Rate Limiting	Indicates that the network is not rate limiting traffic.	0

Exploit

The exploit category indicates events where a communication or access has occurred. The associated low-level event categories include:

Table 13-6 Exploit categories

Low level event category	Description	Severity level (0 to 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 a session in your network has been interceded.	9
Worm Active	Indicates an active worm.	10
Password Guess/Retrieve	Indicates that a user has 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 an 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 has occurred.	9

Table 13-6 Exploit categories (continued)

Low level event category	Description	Severity level (0 to 10)
Cross-Site Scripting	Indicates a cross-site scripting vulnerability.	9
Format String Vulnerability	Indicates a format string vulnerability.	9
Input Validation Exploit	Indicates that an input validation exploit attempt has been detected.	9
Remote Code Execution	Indicates that a remote code execution attempt has been detected.	9
Memory Corruption	Indicates that a memory corruption exploit has been detected.	9
Command Execution	Indicates that a remote command execution attempt has been detected.	9

Malware

The malicious software (malware) category indicates events related to application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 13-7 Malware categories

Low level event category	Description	Severity level (0 to 10)
Unknown Malware	Indicates an unknown virus.	4
Backdoor Detected	Indicates that a backdoor to the system has been 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 a virus has been detected.	8
Misc Malware	Indicates miscellaneous malicious software	4
Trojan Detected	Indicates a trojan has been detected.	7
Spyware Detected	Indicates spyware has been detected on your system.	6
Content Scan	Indicates that an attempted scan of your content has been detected.	3
Content Scan Failed	Indicates that a scan of your content has failed.	8
Content Scan Successful	Indicates that a scan of your content has been successful.	3
Content Scan in Progress	Indicates that a scan of your content is currently in progress.	3

Table 13-7 Malware categories (continued)

Low level event category	Description	Severity level (0 to 10)
Keylogger	Indicates that a key logger has been detected.	7
Adware Detected	Indicates that Ad-Ware has been 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 activity category indicates events related to viruses, trojans, back door attacks, and other forms of hostile software. The associated low-level event categories include:

Table 13-8 Suspicious categories

Low level event category	Description	Severity level (0 to 10)
Unknown Suspicious Event	Indicates an unknown suspicious event.	3
Suspicious Pattern Detected	Indicates a suspicious pattern has been detected.	3
Content Modified By Firewall	Indicates that content has been 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
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

Table 13-8 Suspicious categories (continued)

Low level event category	Description	Severity level (0 to 10)
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 has been 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 QRadar Log Manager 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 a suspicious IP address has been detected.	2
Invalid IP Protocol Usage	Indicates an invalid IP protocol.	2
Invalid Protocol	Indicates an invalid protocol.	4
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 an invalid TCP flag combination has been detected.	5

Table 13-8 Suspicious categories (continued)

Low level event category	Description	Severity level (0 to 10)
Suspicious TCP Flag Combination	Indicates a potentially invalid TCP flag combination has been detected.	4
Illegal ICMP Protocol Usage	Indicates an invalid use of the ICMP protocol has been detected.	5
Suspicious ICMP Protocol Usage	Indicates a potentially invalid use of the ICMP protocol has been detected.	4
Illegal ICMP Type	Indicates an invalid ICMP type has been detected.	5
Illegal ICMP Code	Indicates an invalid ICMP code has been detected.	5
Suspicious ICMP Type	Indicates a potentially invalid ICMP type has been detected.	4
Suspicious ICMP Code	Indicates a potentially invalid ICMP code has been detected.	4
TCP port 0	Indicates a TCP packet using a reserved port (0) for source or destination.	4
UDP port 0	Indicates a UDP packets using a reserved port (0) for source or destination.	4
Hostile IP	Indicates the use of a known hostile IP address.	4
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 should be monitored.	5
Bad Content	Indicates bad content has been detected.	7

Table 13-8 Suspicious categories (continued)

Low level event category	Description	Severity level (0 to 10)
Invalid Cert	Indicates an invalid certificate has been detected.	7
User Activity	Indicates that user activity has been detected.	7
Suspicious Protocol Usage	Indicates suspicious protocol usage has been detected.	5
Suspicious BGP Activity	Indicates that suspicious Border Gateway Protocol (BGP) usage has been detected.	5
Route Poisoning	Indicates that route corruption has been detected.	5
ARP Poisoning	Indicates that ARP-cache poisoning has been detected.	5
Rogue Device Detected	Indicates a rogue device has been detected.	5

System

The system category indicates events related to system changes, software installation, or status messages. The associated low-level event categories include:

Table 13-9 System categories

Low level event category	Description	Severity level (0 to 10)
Unknown System Event	Indicates an unknown system event.	1
System Boot	Indicates a system boot.	1
System Configuration	Indicates a change in the system configuration.	1
System Halt	Indicates the system has been 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 system services have started.	1
Service Stopped	Indicates system services have stopped.	1
Service Failure	Indicates a system failure.	6
Successful Registry Modification	Indicates that a modification to the registry has been successful.	1

Table 13-9 System categories (continued)

Low level event category	Description	Severity level (0 to 10)
Successful Host-Policy Modification	Indicates that a modification to the host policy has been successful.	1
Successful File Modification	Indicates that a modification to a file has been successful.	1
Successful Stack Modification	Indicates that a modification to the stack has been successful.	1
Successful Application Modification	Indicates that a modification to the application has been successful.	1
Successful Configuration Modification	Indicates that a modification to the configuration has been successful.	1
Successful Service Modification	Indicates that a modification to a service has been successful.	1
Failed Registry Modification	Indicates that a modification to the registry has failed.	1
Failed Host-Policy Modification	Indicates that a modification to the host policy has failed.	1
Failed File Modification	Indicates that a modification to a file has failed.	1
Failed Stack Modification	Indicates that a modification to the stack has failed.	1
Failed Application Modification	Indicates that a modification to an application has failed.	1
Failed Configuration Modification	Indicates that a modification to the configuration has failed.	1
Failed Service Modification	Indicates that a modification to the service has failed.	1
Registry Addition	Indicates that an new item has been added to the registry.	1
Host-Policy Created	Indicates that a new entry has been added to the registry.	1
File Created	Indicates that a new has been created in the system.	1
Application Installed	Indicates that a new application has been installed on the system.	1
Service Installed	Indicates that a new service has been installed on the system.	1
Registry Deletion	Indicates that a registry entry has been deleted.	1
Host-Policy Deleted	Indicates that a host policy entry has been deleted.	1
File Deleted	Indicates that a file has been deleted.	1

Table 13-9 System categories (continued)

Low level event category	Description	Severity level (0 to 10)
Application Uninstalled	Indicates that an application has been uninstalled.	1
Service Uninstalled	Indicates that a service has been uninstalled.	1
System Informational	Indicates system information.	3
System Action Allow	Indicates that an attempted action on the system has been authorized.	3
System Action Deny	Indicates that an attempted action on the system has been 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
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 has been 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

Table 13-9 System categories (continued)

Low level event category	Description	Severity level (0 to 10)
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 a client device or authentication server has been 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 hot standby has been enabled successfully.	1
Hot Standby Association Lost	Indicates a hot standby association has been lost.	5
MainMode Initiation Failure	Indicates MainMode initiation failure.	5
MainMode Initiation Succeeded	Indicates that the MainMode initiation has been successful.	1
MainMode Status	Indicates a MainMode status message has been reported.	1
QuickMode Initiation Failure	Indicates that the QuickMode initiation failed.	5
Quickmode Initiation Succeeded	Indicates that the QuickMode initiation has been successful.	1
Quickmode Status	Indicates a QuickMode status message has been 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 has been detected.	5
Service Disruption	Indicates that a service disruption has been detected.	5
License Exceeded	Indicates that the license capabilities have been exceeded.	3
Performance Status	Indicates that the performance status has been reported.	1
Performance Degradation	Indicates that the performance is being degraded.	4

Table 13-9 System categories (continued)

Low level event category	Description	Severity level (0 to 10)
Misconfiguration	Indicates that a incorrect configuration has been detected.	5

Policy

The policy category indicates events related to administration of network policy and the monitoring network resources for policy violations. The associated low-level event categories include:

Table 13-10 Policy categories

Low level event category	Description	Severity level (0 to 10)
Unknown Policy Violation	Indicates an unknown policy violation.	2
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 related to instant messaging (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 indicates events that cannot be otherwise categorized, because they have not been parsed. The associated low-level event categories include:

Table 13-11 Unknown category

Low level event category	Description	Severity level (0 to 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 Pix Firewall event.	3
Unknown Tipping Point Event	Indicates an unknown Tipping Point 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 CRE category indicates events generated from a custom offense, flow or event rule. The associated low-level event categories include:

Table 13-12 CRE category

Low level event category	Description	Severity level (0 to 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 indicates events related to potential application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 13-13 Potential Exploit category

Low level event category	Description	Severity level (0 to 10)
Unknown Potential Exploit Attack	Indicates a potential exploitative attack has been detected.	7
Potential Buffer Overflow	Indicates a potential buffer overflow has been detected.	7
Potential DNS Exploit	Indicates a potentially exploitative attack through the DNS server has been detected.	7
Potential Telnet Exploit	Indicates a potentially exploitative attack through Telnet has been detected.	7
Potential Linux Exploit	Indicates a potentially exploitative attack through Linux has been detected.	7
Potential Unix Exploit	Indicates a potentially exploitative attack through Unix has been detected.	7
Potential Windows Exploit	Indicates a potentially exploitative attack through Windows has been detected.	7
Potential Mail Exploit	Indicates a potentially exploitative attack through mail has been detected.	7
Potential Infrastructure Exploit	Indicates a potential exploitative attack on the system infrastructure has been detected.	7
Potential Misc Exploit	Indicates a potentially exploitative attack has been detected.	7
Potential Web Exploit	Indicates a potentially exploitative attack through the web has been detected.	7
Potential Botnet connection	Indicates a potentially exploitative attack using Botnet has been detected.	6
Potential worm activity	Indicates a potentially attack using worm activity has been detected.	6

User Defined

The User Defined indicates events related to user-defined objects. The associated low-level event categories include:

Table 13-14 Custom category

Low level event category	Description	Severity level (0 to 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
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

Table 13-14 Custom category (continued)

Low level event category	Description	Severity level (0 to 10)
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
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 events category indicates events related to user interaction with the Console and administrative functionality. User login and configuration changes will generate events that are sent to the Event Collector, which correlates with other security events from the network. The associated low-level event categories include:

Table 13-15 SIM Audit Event category

Low level event category	Description	Severity level (0 to 10)
SIM User Authentication	Indicates a user login or logout on the Console.	5
SIM Configuration Change	Indicates that a user has made a change to the SIM configuration or deployment.	3
SIM User Action	Indicates that a user has initiated a process in the SIM module. This might include starting a backup process or generated a report.	3
Session Created	Indicates a user session has been created.	3
Session Destroyed	Indicates a user session has been destroyed.	3
Admin Session Created	Indicates an admin session has been created.	
Admin Session Destroyed	Indicates an admin session has been destroyed.	3
Session Authentication Invalid	Indicates an invalid session authentication.	5
Session Authentication Expired	Indicates a session authentication expired.	3
Risk Manager Configuration	Indicates that a user has made a change to the IBM Security QRadar Risk Manager configuration.	3

VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities 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 associated low-level event categories include:

Table 13-16 VIS Host Discovery category

Low level event category	Description	Severity level (0 to 10)
New Host Discovered	Indicates that the VIS component has detected a new host.	3
New Port Discovered	Indicates that the VIS component has detected a new open port.	3
New Vuln Discovered	Indicates that the VIS component has detected a new vulnerability.	3
New OS Discovered	Indicates that the VIS component has detected a new operating system on a host.	3
Bulk Host Discovered	Indicates that the VIS component has detected many new hosts in a short period of time.	3

Application

The Application category indicates events related to application activity, such as email or FTP activity. The associated low-level event categories include:

Table 13-17 Application category

Low level event category	Description	Severity level (0 to 10)
Mail Opened	Indicates that an email connection has been established.	1
Mail Closed	Indicates that an email connection has been closed.	1
Mail Reset	Indicates that an email connection has been reset.	3
Mail Terminated	Indicates that an email connection has been terminated.	4
Mail Denied	Indicates that an email connection has been denied.	4
Mail in Progress	Indicates that an email connection is being attempted.	1
Mail Delayed	Indicates that an email connection has been delayed.	4
Mail Queued	Indicates that an email connection has been queued.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Mail Redirected	Indicates that an email connection has been redirected.	1
FTP Opened	Indicates that an FTP connection has been opened.	1
FTP Closed	Indicates that an FTP connection has been closed.	1
FTP Reset	Indicates that an FTP connection has been reset.	3
FTP Terminated	Indicates that an FTP connection has been terminated.	4
FTP Denied	Indicates that an FTP connection has been denied.	4
FTP In Progress	Indicates that an FTP connection is currently in progress.	1
FTP Redirected	Indicates that an FTP connection has been redirected.	3
HTTP Opened	Indicates that an HTTP connection has been established.	1
HTTP Closed	Indicates that an HTTP connection has been closed.	1
HTTP Reset	Indicates that an HTTP connection has been reset.	3
HTTP Terminated	Indicates that an HTTP connection has been terminated.	4
HTTP Denied	Indicates that an HTTP connection has been denied.	4
HTTP In Progress	Indicates that an HTTP connection is currently in progress.	1
HTTP Delayed	Indicates that an HTTP connection has been delayed.	3
HTTP Queued	Indicates that an HTTP connection has been queued.	1
HTTP Redirected	Indicates that an HTTP connection has been redirected.	1
HTTP Proxy	Indicates that an HTTP connection is being proxied.	1
HTTPS Opened	Indicates that an HTTPS connection has been established.	1
HTTPS Closed	Indicates that an HTTPS connection has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
HTTPS Reset	Indicates that an HTTPS connection has been reset.	3
HTTPS Terminated	Indicates that an HTTPS connection has been terminated.	4
HTTPS Denied	Indicates that an HTTPS connection has been denied.	4
HTTPS In Progress	Indicates that an HTTPS connection is currently in progress.	1
HTTPS Delayed	Indicates that an HTTPS connection has been delayed.	3
HTTPS Queued	Indicates that an HTTPS connection has been queued.	3
HTTPS Redirected	Indicates that an HTTPS connection has been redirected.	3
HTTPS Proxy	Indicates that an HTTPS connection is proxied.	1
SSH Opened	Indicates than an SSH connection has been established.	1
SSH Closed	Indicates that an SSH connection has been closed.	1
SSH Reset	Indicates that an SSH connection has been reset.	3
SSH Terminated	Indicates that an SSH connection has been terminated.	4
SSH Denied	Indicates that an SSH session has been denied.	4
SSH In Progress	Indicates that an SSH session is currently in progress.	1
RemoteAccess Opened	Indicates that a remote access connection has been established.	1
RemoteAccess Closed	Indicates that a remote access connection has been closed.	1
RemoteAccess Reset	Indicates that a remote access connection has been reset.	3
RemoteAccess Terminated	Indicates that a remote access connection has been terminated.	4
RemoteAccess Denied	Indicates that a remote access connection has been denied.	4
RemoteAccess In Progress	Indicates that a remote access connection is currently in progress.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
RemoteAccess Delayed	Indicates that a remote access connection has been delayed.	3
RemoteAccess Redirected	Indicates that a remote access connection has been redirected.	3
VPN Opened	Indicates that a VPN connection has been opened.	1
VPN Closed	Indicates that a VPN connection has been closed.	1
VPN Reset	Indicates that a VPN connection has been reset.	3
VPN Terminated	Indicates that a VPN connection has been terminated.	4
VPN Denied	Indicates that a VPN connection has been denied.	4
VPN In Progress	Indicates that a VPN connection is currently in progress.	1
VPN Delayed	Indicates that a VPN connection has been delayed	3
VPN Queued	Indicates that a VPN connection has been queued.	3
VPN Redirected	Indicates that a VPN connection has been redirected.	3
RDP Opened	Indicates that an RDP connection has been established.	1
RDP Closed	Indicates that an RDP connection has been closed.	1
RDP Reset	Indicates that an RDP connection has been reset.	3
RDP Terminated	Indicates that an RDP connection has been terminated.	4
RDP Denied	Indicates that an RDP connection has been denied.	4
RDP In Progress	Indicates that an RDP connection is currently in progress.	1
RDP Redirected	Indicates that an RDP connection has been redirected.	3
FileTransfer Opened	Indicates that a file transfer connection has been established.	1
FileTransfer Closed	Indicates that a file transfer connection has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
FileTransfer Reset	Indicates that a file transfer connection has been reset.	3
FileTransfer Terminated	Indicates that a file transfer connection has been terminated.	4
FileTransfer Denied	Indicates that a file transfer connection has been denied.	4
FileTransfer In Progress	Indicates that a file transfer connection is currently in progress.	1
FileTransfer Delayed	Indicates that a file transfer connection has been delayed.	3
FileTransfer Queued	Indicates that a file transfer connection has been queued.	3
FileTransfer Redirected	Indicates that a file transfer connection has been redirected.	3
DNS Opened	Indicates that a DNS connection has been established.	1
DNS Closed	Indicates that a DNS connection has been closed.	1
DNS Reset	Indicates that a DNS connection has been reset.	5
DNS Terminated	Indicates that a DNS connection has been terminated.	5
DNS Denied	Indicates that a DNS connection has been denied.	5
DNS In Progress	Indicates that a DNS connection is currently in progress.	1
DNS Delayed	Indicates that a DNS connection has been delayed.	5
DNS Redirected	Indicates that a DNS connection has been redirected.	4
Chat Opened	Indicates that a chat connection has been opened.	1
Chat Closed	Indicates that a chat connection has been closed.	1
Chat Reset	Indicates that a chat connection has been reset.	3
Chat Terminated	Indicates that a chat connection has been terminated.	3
Chat Denied	Indicates that a chat connection has been denied.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Chat In Progress	Indicates that a chat connection is currently in progress.	1
Chat Redirected	Indicates that a chat connection has been redirected.	1
Database Opened	Indicates that a database connection has been established.	1
Database Closed	Indicates that a database connection has been closed.	1
Database Reset	Indicates that a database connection has been reset.	5
Database Terminated	Indicates that a database connection has been terminated.	5
Database Denied	Indicates that a database connection has been denied.	5
Database In Progress	Indicates that a database connection is currently in progress.	1
Database Redirected	Indicates that a database connection has been redirected.	3
SMTP Opened	Indicates that an SMTP connection has been established.	1
SMTP Closed	Indicates that an SMTP connection has been closed.	1
SMTP Reset	Indicates that an SMTP connection has been reset.	3
SMTP Terminated	Indicates that an SMTP connection has been terminated.	5
SMTP Denied	Indicates that an SMTP connection has been denied.	5
SMTP In Progress	Indicates that an SMTP connection is currently in progress.	1
SMTP Delayed	Indicates that an SMTP connection has been delayed.	3
SMTP Queued	Indicates that an SMTP connection has been queued.	3
SMTP Redirected	Indicates that an SMTP connection has been redirected.	3
Auth Opened	Indicates that an authorization server connection has been established.	1
Auth Closed	Indicates that an authorization server connection has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Auth Reset	Indicates that an authorization server connection has been reset.	3
Auth Terminated	Indicates that an authorization server connection has been terminated.	4
Auth Denied	Indicates that an authorization server connection has been denied.	4
Auth In Progress	Indicates that an authorization server connection is currently in progress.	1
Auth Delayed	Indicates that an authorization server connection has been delayed.	3
Auth Queued	Indicates that an authorization server connection has been queued.	3
Auth Redirected	Indicates that an authorization server connection has been redirected.	2
P2P Opened	Indicates that a Peer-to-Peer (P2P) connection has been established.	1
P2P Closed	Indicates that a P2P connection has been closed.	1
P2P Reset	Indicates that a P2P connection has been reset.	4
P2P Terminated	Indicates that a P2P connection has been terminated.	4
P2P Denied	Indicates that a P2P connection has been denied.	3
P2P In Progress	Indicates that a P2P connection is currently in progress.	1
Web Opened	Indicates that a web connection has been established.	1
Web Closed	Indicates that a web connection has been closed.	1
Web Reset	Indicates that a web connection has been reset.	4
Web Terminated	Indicates that a web connection has been terminated.	4
Web Denied	Indicates that a web connection has been denied.	4
Web In Progress	Indicates that a web connection is currently in progress.	1
Web Delayed	Indicates that a web connection has been delayed.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Web Queued	Indicates that a web connection has been queued.	1
Web Redirected	Indicates that a web connection has been redirected.	1
Web Proxy	Indicates that a web connection has been proxied.	1
VoIP Opened	Indicates that a Voice Over IP (VoIP) connection has been established.	1
VoIP Closed	Indicates that a VoIP connection has been closed.	1
VoIP Reset	Indicates that a VoIP connection has been reset.	3
VoIP Terminated	Indicates that a VoIP connection has been terminated.	3
VoIP Denied	Indicates that a VoIP connection has been denied.	3
VoIP In Progress	Indicates that a VoIP connection is currently in progress.	1
VoIP Delayed	Indicates that a VoIP connection has been delayed.	3
VoIP Redirected	Indicates that a VoIP connection has been redirected.	3
LDAP Session Started	Indicates a LDAP session has started.	1
LDAP Session Ended	Indicates a LDAP session has ended.	1
LDAP Session Denied	Indicates a LDAP session has been denied.	3
LDAP Session Status	Indicates a LDAP session status message has been reported.	1
LDAP Authentication Failed	Indicates a LDAP authentication has failed.	4
LDAP Authentication Succeeded	Indicates a LDAP authentication has been successful.	1
AAA Session Started	Indicates that an Authentication, Authorization and Accounting (AAA) session has started.	1
AAA Session Ended	Indicates that an AAA session has ended.	1
AAA Session Denied	Indicates that an AAA session has been denied.	3
AAA Session Status	Indicates that an AAA session status message has been reported.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
AAA Authentication Failed	Indicates that an AAA authentication has failed.	4
AAA Authentication Succeeded	Indicates that an AAA authentication has been successful.	1
IPSEC Authentication Failed	Indicates that an Internet Protocol Security (IPSEC) authentication has failed.	4
IPSEC Authentication Succeeded	Indicates that an IPSEC authentication has been successful.	1
IPSEC Session Started	Indicates that an IPSEC session has started.	1
IPSEC Session Ended	Indicates that an IPSEC session has ended.	1
IPSEC Error	Indicates that an IPSEC error message has been reported.	5
IPSEC Status	Indicates that an IPSEC session status message has been reported.	1
IM Session Opened	Indicates that an Instant Messenger (IM) session has been established.	1
IM Session Closed	Indicates that an IM session has been closed.	1
IM Session Reset	Indicates that an IM session has been reset.	3
IM Session Terminated	Indicates that an IM session has been terminated.	3
IM Session Denied	Indicates that an IM session has been denied.	3
IM Session In Progress	Indicates that an IM session is in progress.	1
IM Session Delayed	Indicates that an IM session has been delayed	3
IM Session Redirected	Indicates that an IM session has been redirected.	3
WHOIS Session Opened	Indicates that a WHOIS session has been established.	1
WHOIS Session Closed	Indicates that a WHOIS session has been closed.	1
WHOIS Session Reset	Indicates that a WHOIS session has been reset.	3
WHOIS Session Terminated	Indicates that a WHOIS session has been terminated.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
WHOIS Session Denied	Indicates that a WHOIS session has been denied.	3
WHOIS Session In Progress	Indicates that a WHOIS session is in progress.	1
WHOIS Session Redirected	Indicates that a WHOIS session has been redirected.	3
Traceroute Session Opened	Indicates that a Traceroute session has been established.	1
Traceroute Session Closed	Indicates that a Traceroute session has been closed.	1
Traceroute Session Denied	Indicates that a Traceroute session has been 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 has been established.	1
TN3270 Session Closed	Indicates that a TN3270 session has been closed.	1
TN3270 Session Reset	Indicates that a TN3270 session has been reset.	3
TN3270 Session Terminated	Indicates that a TN3270 session has been terminated.	3
TN3270 Session Denied	Indicates that a TN3270 session has been denied.	3
TN3270 Session In Progress	Indicates that a TN3270 session is in progress.	1
TFTP Session Opened	Indicates that a TFTP session has been established.	1
TFTP Session Closed	Indicates that a TFTP session has been closed.	1
TFTP Session Reset	Indicates that a TFTP session has been reset.	3
TFTP Session Terminated	Indicates that a TFTP session has been terminated.	3
TFTP Session Denied	Indicates that a TFTP session has been denied.	3
TFTP Session In Progress	Indicates that a TFTP session is in progress.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Telnet Session Opened	Indicates that a Telnet session has been established.	1
Telnet Session Closed	Indicates that a Telnet session has been closed.	1
Telnet Session Reset	Indicates that a Telnet session has been reset.	3
Telnet Session Terminated	Indicates that a Telnet session has been terminated.	3
Telnet Session Denied	Indicates that a Telnet session has been denied.	3
Telnet Session In Progress	Indicates that a Telnet session is in progress.	1
Syslog Session Opened	Indicates that a syslog session has been established.	1
Syslog Session Closed	Indicates that a syslog session has been closed.	1
Syslog Session Denied	Indicates that a syslog session has been 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 has been established.	1
SSL Session Closed	Indicates that an SSL session has been closed.	1
SSL Session Reset	Indicates that an SSL session has been reset.	3
SSL Session Terminated	Indicates that an SSL session has been terminated.	3
SSL Session Denied	Indicates that an SSL session has been denied.	3
SSL Session In Progress	Indicates that an SSL session is in progress.	1
SNMP Session Opened	Indicates that a Simple Network Management Protocol (SNMP) session has been established.	1
SNMP Session Closed	Indicates that an SNMP session has been closed.	1
SNMP Session Denied	Indicates that an SNMP session has been denied.	3
SNMP Session In Progress	Indicates that an SNMP session is in progress.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
SMB Session Opened	Indicates that a Server Message Block (SMB) session has been established.	1
SMB Session Closed	Indicates that an SMB session has been closed.	1
SMB Session Reset	Indicates that an SMB session has been reset.	3
SMB Session Terminated	Indicates that an SMB session has been terminated.	3
SMB Session Denied	Indicates that an SMB session has been 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 has been established.	1
Streaming Media Session Closed	Indicates that a Streaming Media session has been closed.	1
Streaming Media Session Reset	Indicates that a Streaming Media session has been reset.	3
Streaming Media Session Terminated	Indicates that a Streaming Media session has been terminated.	3
Streaming Media Session Denied	Indicates that a Streaming Media session has been 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 has been established.	1
RUSERS Session Closed	Indicates that a RUSERS session has been closed.	1
RUSERS Session Denied	Indicates that a RUSERS session has been 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 has been established.	1
RSH Session Closed	Indicates that an RSH session has been closed.	1
RSH Session Reset	Indicates that an RSH session has been reset.	3
RSH Session Terminated	Indicates that an RSH session has been terminated.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
RSH Session Denied	Indicates that an RSH session has been 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 has been established.	1
RLOGIN Session Closed	Indicates that an RLOGIN session has been closed.	1
RLOGIN Session Reset	Indicates that an RLOGIN session has been reset.	3
RLOGIN Session Terminated	Indicates that an RLOGIN session has been terminated.	3
RLOGIN Session Denied	Indicates that an RLOGIN session has been 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 has been established.	1
REXEC Session Closed	Indicates that an REXEC session has been closed.	1
REXEC Session Reset	Indicates that an REXEC session has been reset.	3
REXEC Session Terminated	Indicates that an REXEC session has been terminated.	3
REXEC Session Denied	Indicates that an REXEC session has been 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 has been established.	1
RPC Session Closed	Indicates that an RPC session has been closed.	1
RPC Session Reset	Indicates that an RPC session has been reset.	3
RPC Session Terminated	Indicates that an RPC session has been terminated.	3
RPC Session Denied	Indicates that an RPC session has been denied.	3
RPC Session In Progress	Indicates that an RPC session is in progress.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
NTP Session Opened	Indicates that a Network Time Protocol (NTP) session has been established.	1
NTP Session Closed	Indicates that an NTP session has been closed.	1
NTP Session Reset	Indicates that an NTP session has been reset.	3
NTP Session Terminated	Indicates that an NTP session has been terminated.	3
NTP Session Denied	Indicates that an NTP session has been 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 has been established.	1
NNTP Session Closed	Indicates that an NNTP session has been closed.	1
NNTP Session Reset	Indicates that an NNTP session has been reset.	3
NNTP Session Terminated	Indicates that an NNTP session has been terminated.	3
NNTP Session Denied	Indicates that an NNTP session has been 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 has been established.	1
NFS Session Closed	Indicates that an NFS session has been closed.	1
NFS Session Reset	Indicates that an NFS session has been reset.	3
NFS Session Terminated	Indicates that an NFS session has been terminated.	3
NFS Session Denied	Indicates that an NFS session has been 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 has been established.	1
NCP Session Closed	Indicates that an NCP session has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
NCP Session Reset	Indicates that an NCP session has been reset.	3
NCP Session Terminated	Indicates that an NCP session has been terminated.	3
NCP Session Denied	Indicates that an NCP session has been denied.	3
NCP Session In Progress	Indicates that an NCP session is in progress.	1
NetBIOS Session Opened	Indicates that a NetBIOS session has been established.	1
NetBIOS Session Closed	Indicates that a NetBIOS session has been closed.	1
NetBIOS Session Reset	Indicates that a NetBIOS session has been reset.	3
NetBIOS Session Terminated	Indicates that a NetBIOS session has been terminated.	3
NetBIOS Session Denied	Indicates that a NetBIOS session has been denied.	3
NetBIOS Session In Progress	Indicates that a NetBIOS session is in progress.	1
MODBUS Session Opened	Indicates that a MODBUS session has been established.	1
MODBUS Session Closed	Indicates that a MODBUS session has been closed.	1
MODBUS Session Reset	Indicates that a MODBUS session has been reset.	3
MODBUS Session Terminated	Indicates that a MODBUS session has been terminated.	3
MODBUS Session Denied	Indicates that a MODBUS session has been 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 has been established.	1
LPD Session Closed	Indicates that an LPD session has been closed.	1
LPD Session Reset	Indicates that an LPD session has been reset.	3
LPD Session Terminated	Indicates that an LPD session has been terminated.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
LPD Session Denied	Indicates that an LPD session has been 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 has been established.	1
Lotus Notes Session Closed	Indicates that a Lotus Notes session has been closed.	1
Lotus Notes Session Reset	Indicates that a Lotus Notes session has been reset.	3
Lotus Notes Session Terminated	Indicates that a Lotus Notes session has been terminated.	3
Lotus Notes Session Denied	Indicates that a Lotus Notes session has been 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 has been established.	1
Kerberos Session Closed	Indicates that a Kerberos session has been closed.	1
Kerberos Session Reset	Indicates that a Kerberos session has been reset.	3
Kerberos Session Terminated	Indicates that a Kerberos session has been terminated.	3
Kerberos Session Denied	Indicates that a Kerberos session has been 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 has been established.	1
IRC Session Closed	Indicates that an IRC session has been closed.	1
IRC Session Reset	Indicates that an IRC session has been reset.	3
IRC Session Terminated	Indicates that an IRC session has been terminated.	3
IRC Session Denied	Indicates that an IRC session has been denied.	3
IRC Session In Progress	Indicates that an IRC session is in progress.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
IEC 104 Session Opened	Indicates that an IEC 104 session has been established.	1
IEC 104 Session Closed	Indicates that an IEC 104 session has been closed.	1
IEC 104 Session Reset	Indicates that an IEC 104 session has been reset.	3
IEC 104 Session Terminated	Indicates that an IEC 104 session has been terminated.	3
IEC 104 Session Denied	Indicates that an IEC 104 session has been denied.	3
IEC 104 Session In Progress	Indicates that an IEC 104 session is in progress.	1
Ident Session Opened	Indicates that a TCP Client Identity Protocol (Ident) session has been established.	1
Ident Session Closed	Indicates that an Ident session has been closed.	1
Ident Session Reset	Indicates that an Ident session has been reset.	3
Ident Session Terminated	Indicates that an Ident session has been terminated.	3
Ident Session Denied	Indicates that an Ident session has been 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 has been established.	1
ICCP Session Closed	Indicates that an ICCP session has been closed.	1
ICCP Session Reset	Indicates that an ICCP session has been reset.	3
ICCP Session Terminated	Indicates that an ICCP session has been terminated.	3
ICCP Session Denied	Indicates that an ICCP session has been denied.	3
ICCP Session In Progress	Indicates that an ICCP session is in progress.	1
Groupwise Session Opened	Indicates that a Groupwise session has been established.	1
Groupwise Session Closed	Indicates that a Groupwise session has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Groupwise Session Reset	Indicates that a Groupwise session has been reset.	3
Groupwise Session Terminated	Indicates that a Groupwise session has been terminated.	3
Groupwise Session Denied	Indicates that a Groupwise session has been denied.	3
Groupwise Session In Progress	Indicates that a Groupwise session is in progress.	1
Gopher Session Opened	Indicates that a Gopher session has been established.	1
Gopher Session Closed	Indicates that a Gopher session has been closed.	1
Gopher Session Reset	Indicates that a Gopher session has been reset.	3
Gopher Session Terminated	Indicates that a Gopher session has been terminated.	3
Gopher Session Denied	Indicates that a Gopher session has been 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 has been established.	1
GIOP Session Closed	Indicates that a GIOP session has been closed.	1
GIOP Session Reset	Indicates that a GIOP session has been reset.	3
GIOP Session Terminated	Indicates that a GIOP session has been terminated.	3
GIOP Session Denied	Indicates that a GIOP session has been denied.	3
GIOP Session In Progress	Indicates that a GIOP session is in progress.	1
Finger Session Opened	Indicates that a Finger session has been established.	1
Finger Session Closed	Indicates that a Finger session has been closed.	1
Finger Session Reset	Indicates that a Finger session has been reset.	3
Finger Session Terminated	Indicates that a Finger session has been terminated.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Finger Session Denied	Indicates that a Finger session has been denied.	3
Finger Session In Progress	Indicates that a Finger session is in progress.	1
Echo Session Opened	Indicates that an Echo session has been established.	1
Echo Session Closed	Indicates that an Echo session has been closed.	1
Echo Session Denied	Indicates that an Echo session has been 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 has been established.	1
Remote .NET Session Closed	Indicates that a Remote .NET session has been closed.	1
Remote .NET Session Reset	Indicates that a Remote .NET session has been reset.	3
Remote .NET Session Terminated	Indicates that a Remote .NET session has been terminated.	3
Remote .NET Session Denied	Indicates that a Remote .NET session has been 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 has been established.	1
DNP3 Session Closed	Indicates that a DNP3 session has been closed.	1
DNP3 Session Reset	Indicates that a DNP3 session has been reset.	3
DNP3 Session Terminated	Indicates that a DNP3 session has been terminated.	3
DNP3 Session Denied	Indicates that a DNP3 session has been denied.	3
DNP3 Session In Progress	Indicates that a DNP3 session is in progress.	1
Discard Session Opened	Indicates that a Discard session has been established.	1
Discard Session Closed	Indicates that a Discard session has been closed.	1

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
Discard Session Reset	Indicates that a Discard session has been reset.	3
Discard Session Terminated	Indicates that a Discard session has been terminated.	3
Discard Session Denied	Indicates that a Discard session has been 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 has been established.	1
DHCP Session Closed	Indicates that a DHCP session has been closed.	1
DHCP Session Denied	Indicates that a DHCP session has been denied.	3
DHCP Session In Progress	Indicates that a DHCP session is in progress.	1
DHCP Success	Indicates that a DHCP lease has been 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 has been established.	1
CVS Session Closed	Indicates that a CVS session has been closed.	1
CVS Session Reset	Indicates that a CVS session has been reset.	3
CVS Session Terminated	Indicates that a CVS session has been terminated.	3
CVS Session Denied	Indicates that a CVS session has been 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 has been established.	1
CUPS Session Closed	Indicates that a CUPS session has been closed.	1
CUPS Session Reset	Indicates that a CUPS session has been reset.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
CUPS Session Terminated	Indicates that a CUPS session has been terminated.	3
CUPS Session Denied	Indicates that a CUPS session has been 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 has been started.	1
Chargen Session Closed	Indicates that a Chargen session has been closed.	1
Chargen Session Reset	Indicates that a Chargen session has been reset.	3
Chargen Session Terminated	Indicates that a Chargen session has been terminated.	3
Chargen Session Denied	Indicates that a Chargen session has been denied.	3
Chargen Session In Progress	Indicates that a Chargen session is in progress.	1
Misc VPN	Indicates that a miscellaneous VPN session has been detected	1
DAP Session Started	Indicates that a DAP session has been established.	1
DAP Session Ended	Indicates that a DAP session has ended.	1
DAP Session Denied	Indicates that a DAP session has been denied.	3
DAP Session Status	Indicates that a DAP session status request has been made.	1
DAP Session in Progress	Indicates that a DAP session is in progress.	1
DAP Authentication Failed	Indicates that a DAP authentication has failed.	4
DAP Authentication Succeeded	Indicates that DAP authentication has succeeded.	1
TOR Session Started	Indicates that a TOR session has been established.	1
TOR Session Closed	Indicates that a TOR session has been closed.	1
TOR Session Reset	Indicates that a TOR session has been reset.	3

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
TOR Session Terminated	Indicates that a TOR session has been terminated.	3
TOR Session Denied	Indicates that a TOR session has been denied.	3
TOR Session In Progress	Indicates that a TOR session is in progress.	1
Game Session Started	Indicates a game session has started.	1
Game Session Closed	Indicates a game session has been closed.	1
Game Session Reset	Indicates a game session has been reset.	3
Game Session Terminated	Indicates a game session has been terminated.	3
Game Session Denied	Indicates a game session has been denied.	3
Game Session In Progress	Indicates a game session is in progress.	1
Admin Login Attempt	Indicates that an attempt to log in as an administrative user has been detected.	2
User Login Attempt	Indicates that an attempt to log in as a non-administrative user has been 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
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.	

Table 13-17 Application category (continued)

Low level event category	Description	Severity level (0 to 10)
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 indicates audit related events. The associated low-level event categories include:

Table 13-18 Audit categories

Low level event category	Description	Severity level (0 to 10)
General Audit Event	Indicates a general audit event has been started.	1
Built-in Execution	Indicates that a built-in audit task has been run.	1
Bulk Copy	Indicates that a bulk copy of data has been detected.	1
Data Dump	Indicates that a data dump has been detected.	1
Data Import	Indicates that a data import has been detected.	1
Data Selection	Indicates that a data selection process has been detected.	1
Data Truncation	Indicates that the data truncation process has been detected.	1
Data Update	Indicates that the data update process has been detected.	1
Procedure/Trigger Execution	Indicates that the database procedure or trigger execution has been detected.	1
Schema Change	Indicates that the schema for a procedure or trigger execution has been altered.	1

Risk

The Risk category indicates events related to IBM Security QRadar Risk Manager. The associated low-level event categories include:

Table 13-19 Risk categories

Low level event category	Description	Severity level (0 to 10)
Policy Exposure	Indicates a policy exposure has been detected.	5
Compliance Violation	Indicates a compliance violation has been 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
Mis-Configured Rule	Indicates a rule is not configured properly.	3
Mis-Configured Device	Indicates a device on the network is not configured properly.	3
Mis-Configured Host	Indicates a network host is not configured properly.	3
Data Loss Possible	Indicates that the possibility of data loss has been detected.	5
Weak Authentication	Indicates a host or device is susceptible to fraud.	5
No Password	Indicates no password exists.	7
Fraud	Indicates 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 has been detected.	5

Table 13-19 Risk categories (continued)

Low level event category	Description	Severity level (0 to 10)
Policy Monitor Risk Score Accumulation	Indicates that a policy monitor risk score accumulation has been detected.	1

Risk Manager Audit

The Risk Manager Audit category indicates events related to IBM Security QRadar Risk Manager audit events. The associated low-level event categories include:

Table 13-20 Risk Manager Audit category

Low level event category	Description	Severity level (0 to 10)
Policy Monitor	Indicates that a policy monitor has been modified.	3
Topology	Indicates that a topology has been modified.	3
Simulations	Indicates that a simulation has been modified.	3
Administration	Indicates that administrative changes have been made.	3

Control

The Control category indicates events related to your hardware system diagnostics. The associated low-level event categories include:

Table 13-21 Control category

Low level event category	Description	Severity level (0 to 10)
Device Read	Indicates a device has been read.	1
Device Communication	Indicates communication with a device.	1
Device Audit	Indicates a device audit has occurred.	1
Device Event	Indicates a device event has occurred.	1
Device Ping	Indicates a ping action to a device has occurred.	1
Device Configuration	Indicates a device has been configured.	1
Device Route	Indicates a device route action has occurred.	1
Device Import	Indicates a device import has occurred.	1
Device Information	Indicates a device information action has occurred.	1
Device Warning	Indicates a warning has been generated on a device.	1

Table 13-21 Control category (continued)

Low level event category	Description	Severity level (0 to 10)
Device Error	Indicates an error has been 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 an import has occurred.	1
Location Import	Indicates a location import has occurred.	1
Route Import	Indicates a route import has occurred.	1
Export Event	Indicates an export has occurred.	1
Remote Signalling	Indicates remote signalling.	1
Gateway Status	Indicates gateway status.	1
Job Event	Indicates a job has occurred.	1
Security Event	Indicates a security event has occurred.	1
Device Tamper Detection	Indicates that the system has detected a tamper action.	1
Time Event	Indicates that a time event has occurred.	1
Suspicious Behavior	Indicates suspicious behavior has occurred.	1
Power Outage	Indicates a power outage has occurred.	1
Power Restoration	Indicates that power has been restored.	1
Heartbeat	Indicates a heartbeat ping has occurred.	1
Remote Connection Event	Indicates a remote connection to the system.	1

Asset Profiler

The Asset Profiler category indicates events related to asset profiles. The associated low-level event categories include:

Table 13-22 Asset Profiler category

Low level event category	Description	Severity level (0 to 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
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 a operating system was cleaned.	1

Table 13-22 Asset Profiler category (continued)

Low level event category	Description	Severity level (0 to 10)
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
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

Table 13-22 Asset Profiler category (continued)

Low level event category	Description	Severity level (0 to 10)
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
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

Table 13-22 Asset Profiler category (continued)

Low level event category	Description	Severity level (0 to 10)
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
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

C NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

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

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

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

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

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

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

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

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

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM might use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who 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 might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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

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

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

capabilities of non-IBM products should be addressed to the suppliers of those products.

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX

S

T

U

V