IBM Security QRadar Risk Manager
Version 7.2.6

User Guide

IBM

Contents

Introduction to IBM Security QRadar Risk Manager

This information is intended for use with IBM® Security QRadar® Risk Manager. QRadar Risk Manager is an appliance that is used to monitor device configurations, simulate network changes, and prioritize the risks and vulnerabilities in your network.

This guide contains instructions for configuring and using IBM Security QRadar Risk Manager on a IBM Security QRadar SIEM console.

Intended audience

System administrators responsible for configuring and using QRadar Risk Manager must have administrative access to IBM Security QRadar SIEM and to your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

Technical documentation

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

Contacting customer support

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

Statement of good security practices

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

Chapter 1. What's new for users in QRadar Risk Manager V7.2.6

IBM Security QRadar Risk Manager V7.2.6 introduces improvements to help you organize and manage your network topology, filter device rules by users and groups, and new device integrations.

Topology screen enhancements

Manage and organize the topology graph by grouping devices, renaming devices, filtering the number of subnets that are displayed per device, showing or hiding unclassified devices. You can manage the density of network nodes that are displayed by filtering devices and subnets to form an uncluttered graph. Learn more...

Filtering device rules by user or group

To help you manage and optimize your network rule policies, you can view, filter, and search your device rules by user or group. Learn more...

Adapter integrations

QRadar Risk Manager introduces two new adapter integrations that extend the network devices that are supported, such as firewalls, routers, and switches that can be interrogated.

Sidewinder adapter

> QRadar Risk Manager adapter for Sidewinder supports McAfee Enterprise Firewall (Sidewinder) appliances that run SecureOS.

TippingPoint adapter

> QRadar Risk Manager adapter for TippingPoint supports TippingPoint appliances that run TOS and are under SMS control.

For more information, see the *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

Chapter 2. IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network.

QRadar Risk Manager is accessed by using the **Risks** tab on your IBM Security QRadar SIEM Console.

QRadar Risk Manager uses data that is collected by QRadar. For example, configuration data from firewalls, routers, switches, or intrusion prevention systems (IPSs), vulnerability feeds, and third-party security sources. Data sources enable QRadar Risk Manager to identify security, policy, and compliance risks in your network and estimate the probability of risk exploitation.

QRadar Risk Manager alerts you to discovered risks by displaying offenses on the **Offenses** tab. Risk data is analyzed and reported in the context of all other data that QRadar processes. In QRadar Risk Manager you can evaluate and manage risk at an acceptable level that is based on the risk tolerance in your company.

You can also use QRadar Risk Manager to query all network connections, compare device configurations, filter your network topology, and simulate the possible effects of updating device configurations.

You can use QRadar Risk Manager to define a set of policies (or questions) about your network and monitor the policies for changes. For example, if you want to deny unencrypted protocols in your DMZ from the Internet, you can define a policy monitor question to detect unencrypted protocols. Submitting the question returns a list of unencrypted protocols that are communicating from the internet to your DMZ and you can determine which unencrypted protocols are security risks.

Connections

Use the Connections page to monitor the network connections of local hosts.

You can run queries and reports on the network connections of local hosts that are based on any applications, ports, protocols, and websites the local hosts can communicated with.

For more information about Connections, see Investigating connections.

Configuration Monitor

Use Configuration Monitor to review and compare device configuration, allowing you to enforce security policies and monitor device modifications within your network.

Device configurations might include switches, routers, firewalls, and IPS devices in your network. For each device, you can view device configuration history, interfaces, and rules. You can also compare configurations within a device and across devices.

The device configuration information is also used to create the enterprise-wide representation of your network topology, which allows you to determine allowed and denied activity across your network. Device configuration enables you to identify inconsistencies and configuration changes that introduce risk in your network.

Topology

The topology is a graphical representation that depicts the network layer of your network, based on the devices added from Configuration Source Management.

The network layer is layer 3 of the Open Systems Interconnection (OSI) model.

The application layer is layer 7 of the OSI model.

Use the interactive graph in the topology to view connections between devices, virtualized network security devices with multiple contexts, assets, Network Address Translation (NAT) devices, NAT indicators, and information about NAT mappings.

You can search for events, devices, paths, and save network layouts.

You can group devices, and rename devices and groups.

In the topology, you can query the Transport Layer (layer 4) and filter network paths based on port and protocol. The graph and connection information is created from detailed configuration information that is obtained from network devices, such as firewalls, routers, and IPS systems.

For more information, see Topology.

Policy Monitor

Use the policy monitor to define specific questions about risk in your network and submit the question to IBM Security QRadar Risk Manager.

QRadar Risk Manager evaluates the parameters you've defined in your question and returns assets in your network to help you assess risk. The questions are based on a series of tests that can be combined and configured as required. QRadar Risk Manager provides a large number or predefined Policy Monitor questions, and allows the creation of custom questions. Policy Monitor questions can be created for the following situations:

- Communications that have occurred
- Possible communications based on the configuration of firewalls and routers
- Actual firewall rules (device tests)

The Policy Monitor uses data obtained from configuration data, network activity data, network and security events, and vulnerability scan data to determine the appropriate response. QRadar Risk Manager provides policy templates to assist you in determining risk across multiple regulatory mandates and information security best practices, such as PCI, HIPPA, and ISO 27001. You can update the templates to align with your corporate defined information security policies. When the response is complete, you can accept the response to the question and define how you want the system to respond to unaccepted results.

The Policy Monitor allows an unlimited number of questions to be actively monitored. When a question is monitored, QRadar Risk Manager continuously evaluates the question for unapproved results. As unapproved results are discovered, QRadar Risk Manager has the ability to send email, display notifications, generate a syslog event or create an offense in IBM Security QRadar SIEM.

For more information about the Policy Monitor, see Policy Monitor.

Simulations

You use simulations to define, schedule, and perform exploit simulations on your network.

You can create a simulated attack on your topology based on a series of parameters that are configured in a similar manner to the Policy Monitor. You can create a simulated attack on your current network topology, or create a topology model. A topology model is a virtual topology that allows you to make modifications on the virtual topology and simulate an attack. This enables you to simulate how alterations to network rules, ports, protocols, or allowed or denied connections can affect your network. Simulation is a powerful tool to determine the risk impact of proposed changes to your network configuration before the changes are implemented.

After a simulation is complete, you can review the results. If you want to accept the results, you can configure the simulation mode, which allows you to define how you want to respond to unaccepted results.

IBM Security QRadar Risk Manager allows up to 10 simulations to be actively monitored. When a simulation is monitored, QRadar Risk Manager continuously analyzes the topology for unapproved results. As unapproved results are discovered, QRadar Risk Manager has the ability to send email, display notifications, generate a syslog event or create an offense in QRadar SIEM.

For more information about Simulations, see Using simulations.

IBM Security QRadar Risk Manager reports

Use the **Reports** tab to view specific reports, based on data available in QRadar Risk Manager, such as connections, device rules, and device unused objects.

The following additional detailed reports are available:
- connections between devices
- firewall rules on a device
- unused objects on a device

For more information about reports, see Managing IBM Security QRadar Risk Manager reports.

Supported web browsers

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

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

The following table lists the supported versions of web browsers.

Table 1. Supported web browsers for QRadar products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
32-bit Microsoft Internet Explorer, with document mode and browser mode enabled	10.0 11.0
Google Chrome	Version 46

Enabling document mode and browser mode in Internet Explorer

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

Procedure

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode**, and select the **Internet Explorer standards** for your Internet Explorer release.

Access the IBM Security QRadar Risk Manager user interface

IBM Security QRadar Risk Manager uses default login information for the URL, user name, and password.

You access QRadar Risk Manager through the IBM Security QRadar SIEM Console. Use the information in the following table when you log in to your QRadar Console.

Table 2. Default login information for QRadar Risk Manager

Login information	Default
URL	`https://<IP address>`, where *<IP address>* is the IP address of the QRadar Console.
User name	admin
Password	The password that is assigned to QRadar Risk Manager during the installation process.
License key	A default license key provides access to the system for 5 weeks.

Unsupported features in IBM Security QRadar Risk Manager

It is important to be aware of the features that are not supported by QRadar Risk Manager.

The following features are not supported in QRadar Risk Manager:
- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes
- Reference maps
- Store and Forward

Chapter 3. Configure access to QRadar Risk Manager

You can configure access settings for QRadar Risk Manager from the **Admin** tab of IBM Security QRadar SIEM. When you add QRadar Risk Manager to your deployment, you must configure settings, such as the local firewall, network interfaces, email server, and add the appropriate license.

If you have administrator permissions, you can configure several appliance settings for QRadar Risk Manager.

Administrators can do the following tasks:

- From the System and License Management window, you can manage licenses, configure the local firewall, add an email server, and configure network interfaces for QRadar Risk Manager.
- Change the password for a host.
- Update the system time.

Configuring firewall access

Configure IBM Security QRadar Risk Manager local firewall to allow access from specified devices outside of this deployment, that need access to this host. For example, you might want to connect to this host from a computer that is not part of the QRadar setup.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. From the **Display** menu, select **Systems**.
5. Select the host for which you want to configure firewall access settings.
6. From the **Actions** menu, click **View and Manage System**.

   You can right-click the selected host to access this menu option, or you can double-click the host to open the Systems Information window.
7. Click the **Firewall** tab.
8. Configure access for devices that are outside of your deployment, and need to connect to this host.
9. Add this access rule by clicking the arrow.
10. Click **Save**.

Adding your email server for alerts and notifications

You can configure the mail server that is used by QRadar Risk Manager. This is used to distribute alerts and event messages.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.

4. From the **Display** menu, select **Systems**.

5. Select the host for which you want to add an email server address.

6. From the **Actions** menu, select **View and Manage System.**

   Note: You can also right-click the host to access this menu, or you can double-click the host to open the System Information window.

7. Click the **Email Server** tab.

8. In the **Email Server Address** field, type the host name or IP Address of the email server that you want to use.

   Connect your email server through port 25.

   If you don't have an email server and you want to use the email server that QRadar provides, type `localhost`.

9. Click **Save**.

Configuring network interfaces

Configure IP address information and roles for QRadar Risk Manager network interfaces.

Procedure

1. Click the **Admin** tab.

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

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

4. From the **Display** menu, select **Systems**.

5. Select the host on which you want to edit the network interface settings.

6. Click **Actions** > **View and Manage System**, or right-click the selected device to access this menu option. You can also double-click the host to open the System Information window.

7. Click the **Network Interfaces** tab.

8. Select a Network interface from the **Device** column.

9. Click **Edit**.

   You can't edit a network interface with a management, HA crossover, or slave role.

10. Configure the following parameters:
    - The **Role**.
    - IP address attributes.
    - **Move this configuration with active HA** option.

11. Click **Save** to update the settings.

Changing the root password

You can change the root password on your IBM Security QRadar Risk Manager host at regular intervals, or at least every 90 days.

Procedure

1. Use SSH to log in to your QRadar Console as the root user.

2. Type the user name and password for the root user.

   The user name and password are case-sensitive.

3. From your QRadar Console, use SSH to log in to your QRadar Risk Manager as the root user.
4. Use the **passwd** command to change your password.

   The root password does not accept the following special characters: apostrophe ('), dollar sign ($), exclamation mark (!)

Updating the system time

All system time changes must be set on the QRadar Console. Enable time sync services on your QRadar Console and synchronize time with your managed hosts.

About this task

For more information about configuring the system time on your Console, and synchronizing time with managed hosts in your deployment, see the IBM Security QRadar SIEM Administration Guide.

Procedure

1. Use SSH to log in to the QRadar Console as the root user.
2. Edit the `ntp.conf` file.

   `vi /etc/ntp.conf`
3. In the *server* section of the `ntp.conf` file, you can leave the existing server entries or replace them with your own internal (Network Time Protocol) NTP server. Server entries in the `ntp.conf` file begin with `'server'`.

   You can use public servers from the NTP project at (http://www.ntp.org/).

   ```
   server 0.rhel.pool.ntp.org iburst
   server 1.rhel.pool.ntp.org iburst
   server 2.rhel.pool.ntp.org iburst
   server 3.rhel.pool.ntp.org iburst
   ```

   If you use public NTP servers, check that your firewall allows outbound NTP requests.
4. Save changes and close the file.
5. Enable the `ntpd` service to run at run level 3.

   `chkconfig --level 3 ntpd on`
6. Verify that the `ntpd` service is enabled to run at restart.

   `chkconfig --list ntpd`

   Verify that `3:on` displays in the output. This confirms that the service is enabled.

   `ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off`

   You must shut down services before you manually synchronize time with the NTP server.
7. To prevent data collection errors when you change the system time, shut down QRadar services.

   `service hostcontext stop`

   `service tomcat stop`

   `service hostservices stop`
8. Synchronize the time with your NTP server.

   `ntpdate <ntp.server.address>`
9. Start the `ntpd` service.

   `service ntpd start`

10. Restart QRadar services.

   ```
   service hostservices start
   service tomcat start
   service hostcontext start
   ```

11. Synchronize the time on all managed hosts with your QRadar Console by typing the following command.

    ```
    /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
    ```

12. From the **Admin** tab, click **Advanced** > **Deploy Full Configuration**, to restart services on all QRadar managed hosts.

    Time is now synchronized between the QRadar Console and the managed hosts.

Chapter 4. Configuration Source Management

You use Configuration Source Management to configure credentials, add or discover devices, view device configurations, and back up device configurations in IBM Security QRadar Risk Manager.

The data that is obtained from devices in your network is used to populate the topology. You must have administrative privileges to access Configuration Source Management functions from the **Admin** tab in IBM Security QRadar SIEM.

To set up your configuration sources, you must:
1. Configure your device credentials.
2. Discover or import devices. There are two ways to add network devices to QRadar Risk Manager; discover devices using Configuration Source Management or import a list of devices from a CSV file using Device Import.
3. Obtain device configuration from each of your devices.
4. Manage backup jobs to ensure that all updates to device configurations are captured.
5. Set up the discovery schedule to ensure that new devices are automatically discovered.

You use Configuration Source Management to:
- Add, edit, search, and delete configuration sources. For more information, see Manage devices.
- Configure or manage communication protocols for your devices. For more information, see Configure protocols.

If you are using the Juniper NSM device, you must also obtain configuration information.

For detailed information about adapters used to communicate with devices from specific manufacturers, see *IBM Security QRadar Risk Manager Adapter Configuration Guide* .

Credentials

In IBM Security QRadar Risk Manager, credentials are used to access and download the configuration of devices such as firewalls, routers, switches, or IPSs.

Administrators use Configuration Source Management to input device credentials. This provides QRadar Risk Manager access to a specific device. Individual device credentials can be saved for a specific network device. If multiple network devices use the same credentials, you can assign credentials to a group.

For example, if all firewalls in the organization have the same user name and password then the credentials are associated with the address sets for all the firewalls and used to backup device configurations for all firewalls in your organization.

If a network credential is not required for a specific device, the parameter can be left blank in Configuration Source Management. For a list of required adapter credentials, see the *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

You can assign different devices in your network to network groups, allowing you to group together credential and address sets for your devices.

Credential set

A credentials set contains information such as user name, and password values for a set of devices.

Network group

Each network group can include multiple credential and address sets. You can configure your IBM Security QRadar Risk Manager to prioritize how each network group is evaluated.

The network group at the top of the list has the highest priority. The first network group that matches the configured IP address are included as candidates when backing up a device. A maximum of three credential sets from a network group are considered.

For example, if your configuration includes these two network groups:
- Network Group 1 includes two credential sets
- Network Group 2 includes two credential sets

QRadar Risk Manager attempts to compile a list of a maximum of three credential sets. Since Network Group 1 is higher in the list, both of the credential sets in Network Group 1 are added to the list of candidates. Since three credential sets are required, the first credential set in the Network Group 2 is added to the list.

When a credential set successfully accesses a device, QRadar Risk Manager uses that credential set for subsequent attempts to access the device. If the credentials on that device change, the authentication fails when attempting to access the device. Then, on the next authentication attempt, QRadar Risk Manager reconciles the credentials again to ensure success.

Address set

An address set is a list of IP addresses that define a group of devices that share the same set of credentials.

Configuring credentials for IBM Security QRadar Risk Manager

Administrators must configure credentials to allow IBM Security QRadar Risk Manager to connect to devices in the network.

About this task

You can type an IP address range using a dash or wildcard (*) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.*, all IP addresses meeting that requirement are included.

When you configure the address set with Juniper Networks NSM or a generic XML adapter, you must type the IP address range or CIDR address range for all

the devices that are managed by Juniper Networks NSM or files for devices in the repository.

Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. On the navigation menu, click **Credentials**.
5. On the **Network Groups** pane, click the **Add (+)** icon.
6. Type a name for a network group, and then click **OK**.
7. Move the network group that you want to have first priority to the top of the list. You can use the **Move Up** and **Move Down** arrow icons to prioritize a network group.
8. In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click the **Add (+)** icon.

   Repeat for all IP addresses you want to add to the address set for this network group.
9. In the **Credentials** pane, click the **Add (+)** icon.
10. Type a name for the new credential set, and then click **OK**.
11. Type values for the parameters:

Option	Description
Username	Type the user name for the credential set. If you are using a Juniper Networks NSM or a generic XML adapter, type a user name that can access the Juniper NSM server or a user name that can access the file repository that contains your SED (standard element document) files.
Password	Type the password for the credential set. If you are using Juniper Networks NSM or a generic XML adapter, type the password for the Juniper NSM server or the password to log in to the file repository that contains your SED (standard element document) files.
Enable Username	Type the user name for second-level authentication for the credential set.
Enable Password	Type the password for second-level authentication for the credential set.
SNMP Get Community	Type the SNMP Get community.
SNMPv3 Authentication Username	Type the user name you want to use to authenticate SNMPv3.
SNMPv3 Authentication Password	Type the password you want to use to authenticate SNMPv3.
SNMPv3 Privacy Password	Type the protocol you want to use to decrypt SNMPv3 traps.

12. Move the credential set you want to make first priority to the top of the list. Use the **Move Up** and **Move Down** arrow icons to prioritize a credential set.

13. Repeat for each credential set that you want to add.
14. Click **OK**.

Device discovery

The discovery process uses the Simple Networks Management Protocol (SNMP) and command line (CLI) to discover network devices.

After you configure an IP address or CIDR range, the discovery engine performs a TCP scan against the IP address to determine if port 22, 23, or 443 are monitoring for connections. If the TCP scan is successful, and SNMP query is configured to determine the type of device, the SNMP Get Community String is used based on the IP address.

This information is used to determine which adapter the device should be mapped to when added. IBM Security QRadar Risk Manager connects to the device and collects a list of interfaces and neighbor information, such as CDP, NDP, or ARP tables. The device is then added to the inventory.

The configured IP address used to initiate the discovery process might not be the assigned IP address for the new device. QRadar Risk Manager adds a device using the IP address for the lowest numbered interface on the device (or lowest loopback address, if any).

If you use the **Crawl the network from the addresses defined above** check box, the IP address of the neighbors collected from the device are re-introduced into the discovery process and the process repeats for each IP address.

Discovering devices

Administrators use Discover Devices to determine the type of device.

About this task

When performing a device discovery, any device that is not supported but responds to SNMP is added with the Generic SNMP adapter. If you want to perform a path filter through the device with simulated routes, you must manually remove the device.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Configure the SNMP protocol, and add the IP address or CIDR range of the devices that you want to discover.
   a. On the navigation menu, click **Protocols**.
   b. From the Network Groups pane, click the **(+)** symbol.
   c. Type a name for the network group.
   d. Click **OK**.
   e. In the **Add address (IP, CIDR, Wildcard, or Range)** field, type the IP address or CIDR range.
   f. Click **(+)** to add the IP address or CIDR range.
   g. Select the **SNMP** protocol.

h. Click **OK**.
5. On the navigation menu, click **Discover Devices**.
6. Type an IP address or CIDR range.

   This IP address or CIDR range indicates the location of devices you want to discover.
7. Click the **Add (+)** icon.
8. If you want to also search for devices in the network from the defined IP address or CIDR range, select the **Crawl the network from the addresses defined above** check box.
9. Click **Run**.

Import devices

Use Device Import to add a list of adapters and their network IP addresses to the Configuration Source Manager using a comma-separated value file (.CSV).

The device import list can contain up to 5000 devices, but the list must contain one line for each adapter and its associated IP address in the import file.

For example,

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

Where:

`<Adapter::Name>` contains the manufacturer and device name, such as Cisco::IOS.

`<IP Address>` contains the IP address of the device, such as 191.168.1.1.

Table 3. Device import examples

Manufacturer	Name	Example <Adapter::Name>,<IP Address>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importing a CSV file

You can import a master device list to Configuration Source Management using a comma-separated value (CSV) file.

Before you begin

If you import a list of devices and then make a change to an IP address in the CSV file, then you might accidentally duplicate a device in the Configuration Source Management list. For this reason, delete a device from Configuration Source

Management before re-importing your master device list.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Plug-Ins** pane, click **Device Import**.
4. Click **Browse**.
5. Locate your CSV file, click **Open**.
6. Click **Import Devices**.

Results

If an error displays, then you need to review your CSV file to correct errors, and re-import the file. An import of the CSV file might fail if the device list is structured incorrectly or if the device list contains incorrect information. For example, your CSV file might be missing colons or a command, there could be multiple devices on a single line, or an adapter name might have a typo.

If the device import aborts, then no devices from the CSV file are added to Configuration Source Management.

Manage devices

Using the Devices tab in the Configuration Source Management window, you can manage the devices in your network.

From the devices tab, you can view, add, edit, and delete devices. You can also filter the device list, obtain device configuration information, collect neighbor data and discover devices that are in your deployment.

Viewing devices

You can view all the devices in your deployment on the **Devices** tab.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Devices** tab.
5. To view detailed information for a device configuration, select the device you want to view and click **Open**.

Adding a device

You can add individual network devices and adapters using Configuration Source Management.

About this task

You can add an individual device to the device list in Configuration Source Management or you can add multiple devices using a CSV file.

For information about adding multiple devices, see Import devices.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. On the navigation pane, click **Add Device**.
5. Configure values for the following parameters:

Option	Description
IP Address	Type the management IP address of the device.
Adapter	From the **Adapter** drop-down list, select the adapter you want to assign to this device.

6. Click **Add**.

   If necessary, click **Go** to refresh the adapter list.

Editing devices

You can edit a device to correct the IP address or adapter type if there is an error or if your network changed and you need to re-assigned an IP address.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Select the device you want to edit.
5. Click **Edit**.
6. Configure values for the following parameters:

Option	Description
IP Address	Type the management IP address of the device.
Adapter	From the **Adapter** drop-down list, select the adapter you want to assign to this device.

7. Click **Save**.

Deleting a device

You can delete a device from IBM Security QRadar Risk Manager. A deleted device is removed from Configuration Source Management, Configuration Monitor, and the topology.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Devices** tab.
5. Select the device that you want to delete.
6. Click **Remove**.

7. Click **Yes** to delete the device.

Results

After you delete a device, the process to remove the device from the topology might require several minutes.

Filtering the device list

You can use filters to quickly find devices in the device list.

About this task

IBM Security QRadar Risk Manager can handle up to 5000 network devices in Configuration Source Management. Large numbers of network devices can make scrolling through the device list tedious.

The following table describes the types of filters that can be applied to the device list to help you find devices faster.

Table 4. Filter types for the device list

Search Option	Description
Interface IP Address	Filters for devices that have an interface matching either an IP address or CIDR range.
	Type the IP address or CIDR range on which you want to search in the IP/CIDR field.
	For example, if you type a search criteria of 10.100.22.6, the search results return a device with an IP address of 10.100.22.6. If you type a CIDR range of 10.100.22.0/24, all devices in the 10.100.22.* are returned.
Admin IP Address	Filters the device list based on the administrative Interface IP address. An administrative IP address is the IP address that uniquely identifies a device.
	Type the IP address or CIDR range on which you want to search in the **IP/CIDR** field.
OS Version	Filters the device list based on the operating system version devices are running.
	Select values for the following parameters:
	Adapter - Using the drop-down list, select the type of adapter you want to search.
	Version - Using the drop-down list, select the search criteria for the version. For example, greater than, less than, or equal to the specified value. Type the version number in the field on which you want to search. If you do not select a search option for Version, the results include all devices that are configured with the selected adapter, regardless of version.

Table 4. Filter types for the device list (continued)

Search Option	Description
Model	Filters the device list based on the vendor and model number. Configure values for the following parameters: **Vendor** - Using the drop-down list, select the vendor you want to search. **Model** - Type the model you want to search.
Hostname	Filters the device list based on the hostname. Type the host name on which you want to search in the **Hostname** field.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the Risk Manager pane, click **Configuration Source Management**.
4. Click the **Devices** tab.
5. Using the drop-down list to the left side of the device list, select a filter.
6. Click **Go**.

Results

All search results matching your criteria are displayed in the table.

What to do next

To reset a filter, select **Interface IP Address**, clear the **IP/CIDR** address, then click **Go**.

Obtaining device configuration

The process of backing up a device to obtain a device configuration can be completed for a single device in the device list, or you can backup all devices from the **Devices** tab.

About this task

After you configure credential sets and address sets to access network devices, you must backup your devices to download the device configuration so the device information is included in the topology.

For more information about scheduling automated backups of device configurations from the **Jobs** tab, see Manage backup jobs.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.

3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Devices** tab.
5. To obtain the configuration for all devices, click **Backup All** in the navigation pane, and then click **Yes** to continue.
6. To obtain the configuration for one device, select the device. To select multiple devices, hold down the CTRL key and select all necessary devices. Click **Backup**.
7. If necessary, click **View Error** to view the details of an error. After correcting the error, click **Backup All** in the navigation pane.

Collecting neighbor data

Use the discovery process to obtain neighbor data from a device using SNMP and a command line interface (CLI).

About this task

Neighbor data is used in the topology to draw the connection lines to display the graphical topology map of your network devices. The discover button allows you to select single or multiple devices and update the neighbor data for a device. This information is used to update the connection lines for one or many devices in the topology.

Procedure
1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Devices** tab.
5. Select the device for which you want to obtain data. To select multiple devices, hold down the CTRL key and select all necessary devices.
6. Click **Discover**.
7. Click **Yes** to continue.

Results

If you select multiple devices, then the discover process can take several minutes to complete.

What to do next

Select **Run in Background** to work on other tasks.

Manage backup jobs

A job refers to a backup job, which enables you to automatically backup configuration information for all devices in the **Devices** tab on a schedule.

Using the **Jobs** tab from Configuration Source Management, you can create backup jobs for all devices, or individual groups of devices in Configuration Source Management.

Any backup job that you define in the Configuration Source Management page does not affect your IBM Security QRadar SIEM backup configuration using the

Backup and Recovery icon in the **Admin** tab. The backup and recovery functionality obtains configuration information and data for QRadar SIEM. The backup job only obtains information for external devices.

View backup jobs

Jobs and job details are displayed on the **Jobs** tab.

Procedure
1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Jobs** tab.
5. Double-click any job you want to view in greater detail.

Viewing backup job status and logs

You can troubleshoot backup job issues by using the backup status and log file information that is provided on the **Configuration Monitor** page.

About this task

To view backup job status and progress, use the Configuration Monitor page. To view the backup job log file, use the Backup Log Viewer.

Procedure

Go to **Risks** > **Configuration Monitor**. The following columns in the **Device List** table provide information on backup job status:

Column	Description
Backup Status	Indicates the completion status of the backup job: COLLECTED. The backup job is waiting to be processed. RUNNING. The backup job is in progress. SUCCESS. The backup job completed successfully. FAILURE. The backup job did not complete.
Progress	Displays a progress bar that tracks the completion rate of the backup job. To update the progress bar, click the **Refresh** icon on the Configuration Monitor page.
Backup Log	To open the Backup Log Viewer window for the backup job, click the **See Log** link in this column. To update the progress bar, click **Refresh** on the Backup Log Viewer window.

Adding a backup job

You can create backup jobs for all devices, or individual groups of devices in Configuration Source Management.

About this task

After you define the search criteria, you define the job schedule. The schedule configuration displays in the Triggers column. The triggers for a job represent the job schedule. You can have multiple schedules that are configured. For example, you can configure two schedule options so a job runs every Monday and the first of every month.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Jobs** tab.
5. Select **New Job** > **Backup**.
6. Configure values for the following parameters:

Option	Description
Job Name	Type the name you want to apply to this job.
Group	From the Group list, select the group to which you want to assign this job. If there no groups are listed, you can type a group name. You can sort jobs after they are assigned to a group.
Comment	Type any comment you want to associate with this backup job. You can type up to 255 characters in your description of the backup job.

7. Click **OK**.
8. Select one of the following search methods:

Option	Description
Static list	You can use a static list to search for devices by using several options. Using the static list option, you can define the specific devices on which you want to run the job.
Search	Type an IP address or CIDR range that you want to include in the job. When you define the search criteria, the search for devices is performed after the job is run. This ensures that any new devices are included in the job.

9. If you chose Static list, define the search criteria:
   a. Click the **Devices** tab.
   b. From the list on the **Devices** tab, select the search criteria. For more information, see Search criteria for a static list or search.
   c. Click **Go**.
   d. In the **Devices** tab, select the devices that you want to include in the job.
   e. In the Job Details pane, click **Add selected from device view search**.
10. If you chose Search, define the search criteria:

a. Click the **Devices** tab.

b. Using the list in the **Devices** tab, select the search criteria. For more information, see the Search criteria for a static list or search.

c. Click **Go**.

d. In the Job Details pane, click **Use search from devices view**. This search criteria is used to determine devices that are associated with this job.

11. Click **Schedule**, and configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.
Frequency	Select the frequency that you want to associate with this schedule.
Cron	Type a cron expression, which is interpreted in Greenwich Mean Time (GMT). For assistance, contact your administrator.
Specify End Date	Optional. Select a date to end the job schedule.

12. Click **Save** in the Trigger pane.

13. Repeat steps 11 and 12 to create multiple schedules.

14. If you want to run the job immediately, click **Run Now**.

15. Click **Yes** to continue.

Editing a backup job

You can edit backup jobs.

Procedure

1. Click the **Admin** tab.

2. On the navigation menu, click **Plug-ins**.

3. In the **Risk Manager** pane, click **Configuration Source Management**.

4. Click the **Jobs** tab.

5. Double-click the job that you want to edit.

6. Choose one of the following search options from the **Selection Type** parameter:

Option	Description
Static list	A static list enables you to search for devices by using several options. Using the static list option, you can define the specific devices on which you want to run the job.
Search	Type an IP address or CIDR range that you want to include in the job. When you define the search criteria, the search for devices happens after the job is run. This ensures that any new devices are included in the job.

7. If you chose Static List, define the search criteria:

a. Click the **Devices** tab.

b. From the list on the **Devices** tab, select the search criteria.

c. Click **Go**.

d. From the **Devices** tab, select the devices that you want to include in the job.

e. On the **Job Details** pane, click **Add selected from device view search**.

8. If you chose Search, define the criteria:

a. Click the **Devices** tab.

b. Using the list in the **Devices** tab, select the search criteria.

c. Click **Go**.

d. On the Job Details pane, click **Use search from devices view**. This search criteria is used to determine devices that are associated with this job.

9. Click **Schedule**, and configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.
Frequency	Select the frequency that you want to associate with this schedule.
Cron	Type a cron expression, which is interpreted in Greenwich Mean Time (GMT). For assistance, contact your administrator.
Specify End Date	Optional. Select a date to end the job schedule.

10. Click **Save**.

11. Click **Run Now**.

12. Repeat steps 9 and 10, as required.

13. Click **Yes** to continue.

Rename a backup job

You can rename a backup job

Procedure

1. Click the **Admin** tab.

2. On the navigation menu, click **Plug-ins**.

3. In the **Risk Manager** pane, click **Configuration Source Management**.

4. Click the **Jobs** tab.

5. Select the backup job you want to rename.

6. Click **Rename**.

7. Configure values for the following parameters:

Option	Description
Job Name	Type the name you want to apply to this job.

Option	Description
Group	From the **Group** list, select the group to which you want to assign this job. You can also specify a new group name.
Comment	Optional. Type any comment you want to associate with this backup job. You can type up to 255 characters in your description of the backup job.

8. Click **OK**.

Deleting a backup job

You can delete a backup job.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. Click the **Jobs** tab.
5. Select the backup job that you want to delete.
6. Click **Delete**.

Configure protocols

For IBM Security QRadar Risk Manager to communicate with devices, you must define the communication method (protocol) required for communication to your network devices.

QRadar Risk Manager provides default protocol configuration for your system. If you need to define protocols, you can define protocols to allow QRadar Risk Manager to obtain and update device configuration. Many network environments have different communication protocols of different types or functions of the device. For example, a router might use a different protocol than the firewalls in the network. For a list of supported protocols by device manufacturer, see the *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

QRadar Risk Manager uses protocol sets to define groups of protocols for a set of devices that require a specific communication protocol. You can assign devices to network groups, which allows you to group together protocol sets and address sets for your devices.

Protocol sets are a named set of protocols for a set of devices that require specific protocol credentials.

Address sets are IP addresses that define the network group.

Configuring protocols

You define protocols to obtain and update device configuration.

About this task

You can configure the following values for the protocol parameters.

Table 5. Protocol parameters

Protocol	Parameter
SSH	Configure the following parameters: **Port** - Type the port on which you want the SSH protocol to use when communicating with and backing up network devices. The default SSH protocol port is 22. **Version** - Select the version of SSH that you want this network group to use when communicating with network devices. The available options are as follows: **Auto** - This option automatically detects the SSH version to use when communicating with network devices. **1** - Use SSH-1 when communicating with network devices. **2** - Use SSH-2 when communicating with network devices.
Telnet	Type the port number you want the Telnet protocol to use when communicating with and backing up network devices. The default Telnet protocol port is 23.
HTTPS	Type the port number you want the HTTPS protocol to use when communicating with and backing up network devices. The default HTTPS protocol port is 443.
HTTP	Type the port number you want the HTTP protocol to use when communicating with and backing up network devices. The default HTTP protocol port is 80.
SCP	Type the port number you want the SCP protocol to use when communicating with and backing up network devices. The default SCP protocol port is 22.
SFTP	Type the port number you want the SFTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.
FTP	Type the port number you want the FTP protocol to use when communicating with and backing up network devices. The default SFTP protocol port is 22.

Table 5. Protocol parameters (continued)

Protocol	Parameter
TFTP	The TFTP protocol does not have any configurable options.
SNMP	Configure the following parameters: **Port** - Type the port number you want the SNMP protocol to use when communicate with and backing up network devices. **Timeout(ms)** - Select the amount of time, in milliseconds, that you want to use to determine a communication timeout. **Retries** - Select the number of times you want to attempt to retry communications to a device. **Version** - Select the version of SNMP you want to use for communications. The options are v1, v2, or v3. **V3 Authentication** - Select the algorithm you want to use to authenticate SNMP traps. **V3 Encryption** - Select the protocol you want to use to decrypt SNMP traps.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. On the navigation menu, click **Protocols**.
5. Configure a new network group:
    a. In the **Network Groups** pane, click the **Add (+)** icon.
    b. Type a name for a network group.
    c. Click **OK**.
    d. Use the **Move Up** and **Move Down** icons to prioritize the network groups. Move the network group you want to have first priority to the top of the list.
6. Configure the address set:
    a. In the **Add Address** field, type the IP address or CIDR range that you want to apply to the network group, then click the **Add (+)** icon. For example, type an IP address range using a dash or wildcard (*) to indicate a range, such as 10.100.20.0-10.100.20.240 or 1.1.1*. If you type 1.1.1.*, all IP addresses meeting that requirement are included.
    b. Repeat for all IP addresses you want to add to the address set for this network group.
7. Configure the protocol set:
    a. In the **Network Groups** pane, ensure the network group you want to configure protocols for is selected.

b. Select check boxes to apply a protocol to the range of IP addresses assigned to the network group you created. Clearing the check box turns off the communication option for the protocol when attempting to back up a network device.

c. For each protocol that you selected, configure values for the parameters.

d. Use the **Move Up** and **Move Down** icons to prioritize the protocols. Move the protocol that you want to have first priority to the top of the list.

8. Click **OK**.

Configuring the discovery schedule

You can configure a discovery schedule to populate ARP, MAC tables, and neighbor information for your devices. The discovery schedule also allows new devices to be automatically added to the inventory.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Plug-ins**.
3. In the **Risk Manager** pane, click **Configuration Source Management**.
4. On the navigation menu, click **Schedule Discovery**.
5. Select the **Enable periodic discovery** check box to enable schedule discovery.
6. Configure values for the following parameters:

Option	Description
Name	Type a name for the schedule configuration.
Start time	Select a time and date you want to start the backup process. The time must be specified in military time.
Frequency	Select the frequency you want to associate with this schedule.
Cron	Type a cron expression, which is interpreted in Greenwich Mean Time (GMT). For assistance, contact your administrator.
Specify End Date	Optional. Select a date to end the job schedule.
Crawl and discover new devices	Select the check box if you want the discovery process to discover new devices. Clear the check box if you do not want to add new devices to the inventory.

7. Click **OK**.

Chapter 5. Network topology graph

In IBM Security QRadar Risk Manager, you can use the topology model graph to view, filter, and investigate the physical connectivity of your network.

The network topology graph is generated from configuration information that is obtained from devices such as firewalls, routers, switches, and Intrusion Prevention System (IPS) systems. You can hover over connection lines to display network connection information. You can filter the topology by searching for potential attack paths on allowed protocols, ports, or vulnerabilities. You can view the traffic flow between devices or subnets, and you can view device rules.

You can use the topology graph to complete the following tasks:
- Visualize specific network paths and traffic direction for advanced threat analysis.
- Incorporate passive IPS security maps into the topology graph.
- Group devices to organize and simplify the view.
- Add devices to groups, and remove devices from groups.
- Reposition icons in the graph by using your mouse.
- Save topology graph layouts.
- Rename devices and groups.
- Create and save search filters for your network topology that is based on protocols, ports, or vulnerabilities.
- View detailed connection information between devices and subnets.
- View device rules on topology node connections with the allowed ports and protocols.
- View Network Address Translation (NAT) devices, NAT indicators, and information about NAT mappings.
- View virtual Network security devices that have multiple-contexts.

When you search and view the allowed ports and protocols between devices, you can see only connections that use TCP, UDP, and ICMP protocols in the topology graph.

Topology graph searches

Use the topology search feature to view and investigate various elements of your network infrastructure.

You can use the search feature to filter your topology view, and zone in on network paths, hosts, subnets, and other network elements. You can refine your search down to the port or protocol level, for example you can search for potential attack paths on allowed protocols or ports.

You can search events by right-clicking devices and subnets, or search flows by right-clicking subnets.

Click **Actions** to access the **Search** menu. Enter your search criteria in the Search Criteria pane. The following are some of the search options that you can use:

Searching Hosts

If you search for a host, all devices that communicate with that host are displayed. If the host does not match an interface on a device, but is included in the subnet, then that subnet and all connected devices are displayed.

Searching Networks

Search for a single CIDR, for example, `10.3.51.200/24`.

If you're searching for multiple CIDRs, ensure that the CIDRs are valid and are separated by a comma, for example, `10.51.0.0/24,10.51.01/24`.

Searching Paths

A path search displays the traffic direction, fully or partially allowed protocols, and device rules. If port connections exist between networks, the allowed ports are displayed in a path summary.

A **red square** on a connection can indicate network traffic is blocked. If network traffic is moving from node A to node B, then a **red square** on the connection between node A a node B can indicate the following:
- Firewall rules on node B are blocking traffic.
- There is no route on node B to forward packets.

Hover your mouse over the **red square** for more information.

You can search for applications when you select a path in the topology, see Searching for applications. The NAT indicator is a solid **green dot**. This is displayed in the topology graph when the search returns a path that contains source or destination translations.

From the **Actions** menu, you can access the **Search** menu.

Searching for applications

Search for applications from the IBM Security QRadar Risk Manager topology from the **Risks** tab, or when you select a path in the topology, to view application details.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Click **Search** > **New Search**.
4. Select the **Path** option.
5. Click **Select Applications**.
6. In the **Device Adapter** drop-down menu, select the required device adapter type.
7. In the **Application Name** field, enter the descriptor for the application.
8. Click **Search**.
9. Click each application that you want to search on in the **Search Results** field, and click **Add**.
10. Click **OK**.

Searching by vulnerabilities

You can search by vulnerabilities from the **Search** menu if you have an intrusion prevention system (IPS) placed in your Topology graph.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Click **Search** > **New Search**.
4. Select the **Path** option.
5. Click **Select Vulnerability**.
6. From the **Search By** menu, select the vulnerability category.
7. In the **Field** beside the **Search By** menu, enter the ID number of the vulnerability.
8. Click **Search**.
9. Click each vulnerability that you want to search on in the **Search Results** field, and click **Add**.
10. Click **Save**.
11. Click **Search** to view results.

    See Add an intrusion prevention system (IPS), if you don't see the vulnerability search option.

NAT indicators in search results

A NAT indicator, which is a solid green dot, displays in the topology graph if your search finds a path that contains source or destination translations.

About this task

A NAT indicator indicates that the destination IP address that was specified in the path filter might not be the final destination. Hover over the indicator to view the following information about the translations.

Table 6. Information available from the NAT indicator

Parameter	Description
Source	The translated source IP or CIDR.
Source Port(s)	The translated source ports, if applicable.
Translated Source	The result of the translation that was applied to the source.
Translated Source Port(s)	The result of the translation that was applied to the source port(s), if applicable.
Destination	The translated destination IP or CIDR.
Destination Port(s)	The translated destination ports, if applicable.
Translated Destination	The result of the translation that was applied to the destination.
Translated Destination Port(s)	The result of the translation that was applied to the destination port(s), if applicable.

Table 6. Information available from the NAT indicator (continued)

Parameter	Description
Phase	The routing phase when the translation was applied. Translations are applied either pre- or post-routing.

Add an intrusion prevention system (IPS)

If your **Configuration Source Management** list includes an intrusion prevention system (IPS) device, you can add an IPS to connections between a device-to-subnet nodes, and between device-to-device nodes.

About this task

Adding an IPS connection is useful to determine the location of the IPS if the device is passive.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Move your mouse pointer over the connection line that links a device node and a subnet node.
4. Right-click the connection line, select **Add IPS**.
5. Select the device and interfaces to add from the following lists:

Option	Description
Place IPS	Select a placement from the list.
Connect IPS interface	Select an interface to connect to the device. If there are multiple choices devices, then you need to select a device (see next option).
to device	Select the device that you want to connect to the IPS. This option is available if there are multiple devices.
Connect IPS interface	Select an interface to connect to the subnet.

6. Using the lists, select the device and interfaces to add the IPS connection to your topology.
7. Click **OK**. If you want to add an IPS to a device that is in a group, expand the group to add the IPS.

Remove an Intrusion Prevention System (IPS)

You can remove an IPS connection.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Topology**.
3. Move your mouse pointer over the connection line that links a device node and a subnet node.
4. Right-click the connection line, select the Remove IPS idp option.
5. Click **OK**.

Topology device groups

Group devices in a Topology page to organize and simplify complicated topology graphs.

Select a device in the Current Topology window and click the **Actions** menu on the toolbar, or use the right-click menu to access the device **Groups** feature.

Topology graph layout

Save your topology layout as your current view. When you save your layout, you are saving the current graphical representation of the topology.

The saved layout remains the default topology screen, until you reset the layout, by clicking **Actions** > **Layout** > **Reset Layout**.

When you reset a layout, select **Save Layout** if you want to retain this layout.

Download the current topology as a PNG image or a VDX (Microsoft Visio 2010) drawing, by clicking **Actions** > **Download**.

Chapter 6. Policy Monitor

Organizations use Policy Monitor to define specific risk questions about the network to assess or monitor risk that is based on the analysis of risk indicators.

In Policy Monitor, you can define policies, assess adherence to a policy, evaluate results of questions, and monitor new risks.

Default question templates are provided for you to assess and monitor the risk on your network. You can use one of the default question templates as a basis for your own questions or you can create a new question. You can find the default question templates in the **Group** menu on the Policy Monitor page.

You can choose from the following list of risk indicators:
- Network activity measures risk based on network communications that occurred in the past.
- Configuration and topology measure risk that is based on possible communication and network connections.
- Vulnerabilities measure risk that is based on your network configuration and vulnerability scan data that is collected from network assets.
- Firewall rules measures risk based on the enforcement or absence of firewall rules that are applied across the network.

You can define tests that are based on the risk indicators, and then restrict the test results to filter the query for specific results or violations.

Security professionals create questions for assets or devices/rules to flag risks in their networks. The risk level for an asset or a device/rule is reported after a question is submitted to the Policy Monitor. You can approve results that are returned from assets or define how you want the system to respond to unapproved results.

You can use the results to assess risk cases for many varied security scenarios, for example:
- Assess if users used forbidden protocols to communicate.
- Assess if users, on specific networks, can communicate to forbidden networks or assets.
- Assess if firewall rules meet corporate policy.
- Prioritize vulnerabilities by assessing which systems can be compromised as a result of network configuration.

Policy Monitor questions

You can define questions in Policy Monitor to assess and monitor risk based on network activity, vulnerabilities, and firewall rules.

When you submit a question, the topology search is based on the data type that you selected:
- For questions based on assets, then the search is based on the network assets that violated a defined policy or assets that introduced risk into the network.

- For questions based on devices/rules, then the search either identifies the rules in a device that violated a defined policy or introduced risk into the network.
- If a question is based on asset compliance, then the search identifies if an asset is compliant with a CIS benchmark.

Note: If you configured IBM Security QRadar for multiple domains, asset questions only monitor assets in your default domain. Asset compliance questions monitor assets in your default domain unless you configured another domain in the **Admin** > **Domain Management** window. For more information about domain management, see the *IBM Security QRadar SIEM Administration Guide*.

Devices/rules questions look for violations in rules and policy and do not have restrictive test components. You can also ask devices/rules questions for applications.

Asset tests are divided into these categories:

- A *contributing test* uses the question parameters to examine the risk indicators that are specified in the question. Risk data results are generated, which can be further filtered using a *restrictive test*. Contributing tests are shown in the **Which tests do you want to include in your question** area. Contributing tests return data based on assets detected that match the test question.
- A *restrictive test* narrows the results that are returned by a *contributing test* question. Restrictive tests display only in the **Which tests do you want to include in your question** area after a contributing test is added. You can add restrictive tests only after you include a contributing test in the question. If you remove or delete a contributing test question, the restrictive test question cannot be saved.

Asset compliance questions look for assets that are not in compliance with CIS benchmarks. The tests that are included in the CIS benchmark are configured with the Compliance Benchmark Editor.

Related tasks:

"Submitting a question" on page 41
You submit a question to determine the associated risk. You can also determine the time that is required to run a question and the amount of data that is queried.

"Editing a compliance benchmark" on page 42
Use the Compliance Benchmark Editor in IBM Security QRadar Risk Manager to add or remove tests from the default CIS benchmarks.

Importance factor

The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.

The range is 1 (low importance) to 10 (high importance). The default is 5.

Table 7. Importance factor results matrix

Importance Factor	Returned Results for Asset Tests	Returned Results for Device/Rule Tests
1 (low importance)	10,000	1,000
10 (high importance)	1	1

For example, a policy question that states **have accepted communication from the internet and include only the following networks (DMZ)** would require a high importance factor of 10 since any results to the question is unacceptable due to the high risk nature of the question. However, a policy question that states have accepted communication from the internet and include only the following inbound applications (P2P) might require a lower importance factor since the results of the question does not indicate high risk but you might monitor this communication for informational purposes.

View question information

You can view information about Policy Monitor questions and parameters on the Policy Monitor page.

If you want to view more information about any question, then you can select the question to view the description.

If a question is in monitor mode when you select it, then you can view the events and offenses that are generated as a result of the selected question.

Creating an asset question

Search for assets in the network that violate a defined policy or assets that introduced risk.

About this task

Policy Monitor questions are evaluated in a top-down manner. The order of Policy Monitor questions impacts the results.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Asset Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. From the **Evaluate On** list, select one of the following options:

Option	Description
Actual Communication	Includes any assets on which communications were detected that use connections.
Possible Communication	Includes any assets on which communications are allowed through your network topology, such as firewalls. You use these questions to investigate whether specific communications are possible, regardless of whether a communication was detected.

6. From the **Importance Factor** list, select the level of importance you want to associate with this question. The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.
7. Specify the time range for the question.

8. From the **Which tests do you want to include in your question** field, select the add (+) icon beside the tests you want to include.
9. Configure the parameters for your tests in the **Find Assets that** field.

   Configurable parameters are bold and underlined. Click each parameter to view the available options for your question.
10. In the groups area, click the relevant check boxes to assign group membership to this question.
11. Click **Save Question**.

What to do next

Submit a question to determine the risk factor. See "Submitting a question" on page 41.

Related concepts:

"Importance factor" on page 38
The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.

"Group questions" on page 53
You can group and view your questions based on your chosen criteria

Creating a question that tests for rules in devices

Create a devices/rules question in Policy Monitor to identify the rules in a device that violated a defined policy, or introduced risk into the network.

About this task

Policy Monitor questions are evaluated in a top down manner. The order of Policy Monitor questions impacts the results.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, click **New Device/Rules Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. From the **Importance Factor** list, select the level of importance that you want to associate with this question.
6. From the **Which tests do you want to include in your question** field, click the + icon beside the tests you want to include.
7. In the **Find Devices/Rules that** field, configure the parameters for your tests.

   Configurable parameters are bold and underlined. Click each parameter to view the available options for your question.
8. In the groups area, click the relevant check boxes to assign group membership to this question.
9. Click **Save Question**.

What to do next

Submit a question to determine the risk factor.

Related concepts:

"Importance factor" on page 38
The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.

"Group questions" on page 53
You can group and view your questions based on your chosen criteria

Related tasks:

"Submitting a question"
You submit a question to determine the associated risk. You can also determine the time that is required to run a question and the amount of data that is queried.

Submitting a question

You submit a question to determine the associated risk. You can also determine the time that is required to run a question and the amount of data that is queried.

About this task

When you submit a question, the resulting information depends on the data that is queried; assets or devices and rules.

After a Policy Monitor question is submitted, you can view how long the question takes to run. The time that is required to run the policy also indicates how much data is queried. For example, if the execution time is 3 hours then there is 3 hours of data. You can view the time in the **Policy Execution Time** column to determine an efficient interval frequency to set for the questions that you want to monitor. For example, if the policy execution time is 3 hours, then the policy evaluation interval must be greater than 3 hours.

Note: When you edit a question after it is submitted, and the edit affects associated tests, then it might take up to an hour to view those changes.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question that you want to submit.
4. Click **Submit Question**.

Creating an asset compliance question

Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Before you begin

Policy Monitor questions are evaluated in a top down manner. The order of Policy Monitor questions impacts the results.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Asset Compliance Question**.
4. In the **What do you want to name this question** field, type a name for the question.

5. Select the level of importance you want to associate with this question from the **Importance Factor** list.

6. From the **Which tests do you want to include in your question** field, select the add (+) icon beside the **test compliance of assets in asset saved searches with CIS benchmarks** test.

   Select this test multiple times, if necessary.

7. Configure the parameters for your tests in the **Find Assets that** field.

   Click each parameter to view the available options for your question. Specify multiple assets saved searches and multiple checklists in this test, if necessary.

8. In the group area, click the relevant check boxes to assign group membership to this question.

   Asset compliance questions must be assigned to a group for inclusion in compliance dashboards or reports.

9. Click **Save Question**.

What to do next

Associate a benchmark profile with, and monitor the results of, the question you created.

Related concepts:

"Importance factor" on page 38
The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.

"Group questions" on page 53
You can group and view your questions based on your chosen criteria

Related tasks:

"Monitoring asset compliance questions" on page 43
Monitor asset compliance questions by selecting CIS scan profiles. CIS benchmark scans run against the assets.

Editing a compliance benchmark

Use the Compliance Benchmark Editor in IBM Security QRadar Risk Manager to add or remove tests from the default CIS benchmarks.

Procedure

1. Click the **Risks** tab.

2. Click **Policy Monitor**.

3. Click **Compliance** to open the Compliance Benchmark Editor window.

4. On the navigation menu, click the default CIS benchmark that you want to edit.

5. In the **Compliance** pane, click the **Enabled** check box in the row that is assigned to the test that you want to include.

   Click anywhere on a row to see a description of the benchmark test, a deployment rationale, and information on things to check before you enable the test.

   When you are building a custom CIS checklist, be aware that some benchmark tests that are not included by default can take a long time to run. For more information, please refer to the CIS documentation.

What to do next

Create an asset compliance question to test assets against the benchmark you edited.

Related tasks:

"Creating an asset compliance question" on page 41
Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Monitoring asset compliance questions

Monitor asset compliance questions by selecting CIS scan profiles. CIS benchmark scans run against the assets.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. In the **Questions** pane, select the asset compliance question that you want to monitor.
4. Click **Monitor** to open the Monitor Results window.
5. Select a benchmark profile from the **Which benchmark profile to associate with this question?** list.

   The selected benchmark scan profile uses a QRadar Vulnerability Manager scanner that is associated with a domain. The domain name is displayed in the **Benchmark Profile Details** area. For more information about domain management, see the *IBM Security QRadar SIEM Administration Guide*.
6. Select the **Enable the monitor results function for this question/simulation** check box.
7. Click **Save Monitor**.

   Monitoring begins at the scan start time that you set on the **When To Scan** tab when you created the benchmark scan profile.

Related tasks:

"Editing a compliance benchmark" on page 42
Use the Compliance Benchmark Editor in IBM Security QRadar Risk Manager to add or remove tests from the default CIS benchmarks.

"Creating an asset compliance question" on page 41
Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Export and import policy monitor questions

Users with administrative privileges can export and import Policy Monitor questions.

Exporting and importing questions provides a method to back up questions and share questions with other IBM Security QRadar Risk Manager users.

Restrictions for sensitive information

Sensitive company or policy information might be included in dependencies. When you export or import Policy Monitor questions, the sensitive data contained in the dependencies is not included.

Policy monitor questions might contain the following types of dependencies:
* Asset building blocks
* Asset saved searches
* Networks
* Remote network locations
* Geographic network locations
* Reference sets

Before you export questions that have dependencies, you might choose to provide more context about the type of information that is contained in the dependency. Providing this information allows other users to understand what type of information to reference when they import the question in their Policy Monitor.

Exporting policy monitor questions

You can export one or more of your policy monitor questions to an XML file. Exporting policy monitor questions is useful for backing up your questions or sharing questions with other users.

About this task

If any policy monitor questions contain dependencies, then you can provide more context about the type of information that is contained in the dependency.

The default XML file name for the exported questions is `policy_monitor_questions_export.xml`.

Procedure

1. On the **Risks** tab, click **Policy Monitor**.
2. Choose one of the following options:
   * To export all questions, from the **Actions** menu, select **Export All**.
   * To export select questions, press the Ctrl key to select each question that you want to export and then from the **Actions** menu, select **Export Selected**.
3. Optional. If any questions contain dependencies, then click the parameter link to type more specific information. The maximum character length for this field is 255.
4. Click **Export Questions**.

Results

A default file, called `policy_monitor_questions_export.xml`, is exported to your download directory.

Importing policy monitor questions

You can import one or more policy monitor questions to IBM Security QRadar Risk Manager.

About this task

The import process does not update existing questions; each question displays as a new question in policy monitor. A timestamp is added, as a suffix, to all imported questions.

After you import policy monitor questions, a warning displays in the **Status** column if an imported question contains a dependency. Imported questions with dependencies contain parameters without values. To ensure that imported policy monitor questions work as expected, you must assign values to empty parameters.

Procedure

1. On the **Risks** tab, click **Policy Monitor**.
2. From the **Actions** menu, select **Import**.
3. Click **Choose File**, and then browse to select the XML file that you want to import.
4. Click **Open**.
5. Select one or more groups to assign the question to a group.
6. Click **Import Question**.
7. Check the **Status** column for warnings. If a question contains a warning, open the question and edit the dependent parameters. You can save the question after the parameters are complete.

What to do next

Monitoring is disabled for imported questions. You can create an event to monitor results of questions that were imported.

Asset results

Asset results display after you submit a policy monitor question.

The **Risk Score** indicates the level of risk that is associated with the question. The **Risk Score** calculation is based on the importance factor assigned to the question, and the number of results returned for the question.

The parameters for asset results are described in the following table.

Table 8. Asset results

Parameter	Description
IP	The IP address of the asset.
Name	The name of the asset, as obtained from the asset profile. For more information about asset profiles, see the *IBM Security QRadar SIEM Users Guide*
Vlan	The name of the VLAN associated with the asset.
Weight	The weight of the asset, as obtained from the asset profile.

Table 8. Asset results (continued)

Parameter	Description
Destination Port(s)	The list of destination ports associated with this asset, in context of the question tests. If there are multiple ports associated with this asset and question, this field indicates Multiple and the number of multiple ports. The list of ports is obtained by filtering the connections associated with this question to obtain all unique ports where the asset has either been the source, destination, or the connection.
	Click Multiple (N) to view the connections. This display provides the aggregated connections by port, filtered by the asset IP address, and based on the time interval specified in the question.
Protocol(s)	The list of protocols associated with this asset, in context of the question tests. If there are multiple protocols associated with this asset and question, this field indicates Multiple and the number of protocols. The list of protocols is obtained by filtering the connections associated with this question to obtain all unique protocols where the asset has either been the source, destination, or the connection.
	Click Multiple (N) to view the Connections. This display provides the aggregated connections by protocol, filtered by the asset IP address, and based on the time interval specified in the question.
Flow App(s)	The list of applications associated with this asset, in context of the question tests. If there are multiple applications associated with this asset and question, this field indicates Multiple and the number of applications. The list of applications is obtained by filtering the connections associated with this question to obtain all unique applications where the asset has either been the source, destination, or the connection.
	Click Multiple (N) to view the Connections. This display provides the aggregated connections by application, filtered by the asset IP address, and based on the time interval specified in the question.

Table 8. Asset results (continued)

Parameter	Description
Vuln(s)	The list of vulnerabilities associated with this asset, in context of the question tests. If there are multiple vulnerabilities associated with this asset and question, this field indicates Multiple and the number of vulnerabilities. The list of vulnerabilities is obtained using a list of all vulnerabilities compiled from relevant tests and using this list to filter the vulnerabilities detected on this asset. If no vulnerabilities are specified for this question, then all vulnerabilities on the asset are used to compile this list. Click Multiple (N) to view the Assets. This display provides the aggregated connections by vulnerability, filtered by the asset IP address, and based on the time interval specified in the question.
Flow Count	The total flow count associated with this asset, in context of the question tests. The flow count is determined by filtering the connections associated with this question to obtain the flow count total, where asset has either been the source, destination, or the connection.
Source(s)	The list of source IP addresses associated with this asset, in context of the question tests. If there are multiple source IP addresses associated with this asset and question, this field indicates Multiple and the number of source IP addresses. The list of source IP addresses is obtained by filtering the connections associated with this question to obtain all unique source IP addresses where the asset is the destination of the connection. Click Multiple (N) to view the Connections. This display provides the aggregated connections by source IP address filtered by the asset IP address based on the time interval specified in the question.

Table 8. Asset results (continued)

Parameter	Description
Destination(s)	The list of destination IP addresses associated with this asset, in context of the question tests. If there are multiple destination IP addresses associated with this asset and question, this field indicates Multiple and the number of destination IP addresses. The list of destination IP addresses is obtained by filtering the connections associated with this question to obtain all unique destination IP addresses where the asset is the source of the connection. Click Multiple (N) to view the Connections. This display provides the aggregated connections by destination IP address filtered by the asset IP address based on the time interval specified in the question.
Flow Source Bytes	The total source bytes associated with this asset, in context of the question test. The source bytes is determined by filtering the connections associated with this question to obtain the source byte total where asset is the source of the connection.
Flow Destination Bytes	The total destination bytes associated with this asset, in context of the question test. The destination bytes is determined by filtering the connections associated with this question to obtain the destination byte total where asset is the destination of the connection.

Device/Rule results

Device/Rule results display after you submit a policy monitor question.

The **Risk Score** displayed indicates the level of risk that is associated with the question. The **Risk Score** calculation is based on the importance factor assigned to the question, and the number of results returned for the question.

The parameters for devices and rules results are described in the following table.

Table 9. Devices and rules results

Parameter	Description
Device IP	The IP address of the device.
Device Name	The name of the device, as obtained from the configuration monitor.
Device Type	The type of device, as obtained from the asset profile. For more information about asset profiles, see the *IBM Security QRadar SIEM Users Guide*.

Table 9. Devices and rules results (continued)

Parameter	Description
List	The name of the rule from the device.
Entry	The entry number of the rule.
Action	The action associated with the relevant rule from the device. The options are: permit, deny, or NA.
Source(s)	The source network associated with this asset. Sources with a hyperlink indicate an object group reference. Click the link to view detailed information about the object group reference(s).

Source Service(s)	The source ports and the comparison associated with the relevant rule from the device in the following format:
	
	`<comparison>:<port>`
	
	Where
	
	`<comparison>`
	
	could include one of the following options:
	
	eq - Equal
	
	ne - Not equal
	
	lt - Less than
	
	gt - Greater than
	
	For example, if the parameter indicates ne:80, any port other than 80 applies to this source service. If the parameter indicates lt:80, the range of applicable ports is 0 to 79.
	
	This parameter displays the source port for the device rule. If no port exists for this device rule, the term NA is displayed.
	
	Source services with a hyperlink indicate an object group reference. Click the link to view detailed information about the object group reference(s).

Destination(s)	The destination network associated with the relevant rule from the device. Destinations with a hyperlink indicate an object group reference. Click the link to view detailed information about the object group reference(s).

Table 9. Devices and rules results (continued)

Parameter	Description

Destination Service(s)	The destination ports and the comparison associated with the relevant rule from the device is displayed in the following format:
	
	`<comparison>:<port>`
	
	Where
	
	`<comparison>`
	
	might include one of the following options:
	
	eq - Equal
	
	ne - Not equal
	
	lt - Less than
	
	gt - Greater than
	
	For example, if the parameter indicates ne:80, any port other than 80 applies to this destination service. If the parameter indicates lt:80, the range of applicable ports is 0 to 79.
	
	This parameter displays the destination port for the device rule. If no port exists for this device rule, the term NA is displayed.
	
	Destination services with a hyperlink indicate an object group reference. Click the link to view detailed information about the object group reference(s).

User(s)Group(s)	The users or groups associated with the relevant rule from the device.
Protocol(s)	The protocol or group of protocols associated with the relevant rule from the device.
Signature(s)	The signature for this device, which is only displayed for a device rule on an IP device.
Applications	The applications that are associated with the relevant rule from the device.

Evaluate results of Policy Monitor questions

You can evaluate the results that are returned from a Policy Monitor question.

Approving a result of a question is similar to tuning your system to inform IBMIBM Security QRadar Risk Manager that the asset associated with the question result is safe or can be ignored in the future.

When a user approves an asset result, the Policy Monitor sees that asset result as approved, and when the Policy Monitor question is submitted or monitored in the future, the asset is not listed in the question results. The approved asset does not display in the results list for the question unless the approval is revoked. The

Policy Monitor records the user, IP address of the device, reason for approval, the applicable Device/Rule, and the date and time for your network security administrators.

Approving results

You can evaluate the list of assets or device rules returned to determine the level of risk involved. After you evaluate, you might approve all or specific results.

Procedure

1. In the results table, select the check box next to the results you want to accept.
2. Choose one of the following options:

Option	Description
Approve All	Select this option to approve all the results.
Approve Selected	Select the check box next to the results that you want to approve, and then click Approve Selected.

3. Type the reason for approval.
4. Click **OK**.
5. Click **OK**.
6. To view the approved results for the question, click **View Approved**.

Results

The Approved Question Results window provides the following information:

Table 10. Approved question results parameters

Parameter	Description
Device/Rule	For a Device/Rule question result, this indicates the device associated with this result.
IP	For an asset question result, this indicates the IP address associated with the asset.
Approved By	The user that approved the results.
Approved On	The date and time the results were approved.
Notes	Displays the text of notes associated with this result and the reason the question was approved.

If you want to remove approvals for any result, select the check box for each result for which you want to remove approval and click **Revoke Selected**. To remove all approvals, click **Revoke All**.

Monitor questions

If you want to generate an event when the results of a question change, you can configure a question to be monitored.

When you select a question to be monitored, IBM Security QRadar Risk Manager continually analyzes the question to determine if the results of a question change.

If QRadar Risk Manager detects a result change, an offense can be generated to alert you to a deviation in your defined policy.

A question in monitor mode defaults to a time range of 1 hour. This value overrides the time value that is set when the question was created.

Creating an event to monitor results

You can create an event to monitor results of questions that were created in Policy Monitor.

About this task

The parameters that you configure for an event are described in the following table.

Table 11. Monitor question results parameters

Parameter	Description
Policy evaluation interval	The frequency for the event to run.
Event Name	The name of the event you want to display in the **Log Activity** and **Offenses** tabs.
Event Description	The description for the event. The description is displayed in the Annotations of the event details.
High-Level Category	The high-level event category you want this rule to use when processing events.
Low-Level Category	The low-level event category you want this rule to use when processing events.
Ensure the dispatched event is part of an offense	Forwards the events to the Magistrate component. If no offense has been generated, a new offense is created. If an offense exists, the event is added. If you correlate by question or simulation, then all events from a question are associated to a single offense. If you correlate by asset, then a unique offense is created or updated for each unique asset.
Dispatch question passed events	Forwards events that pass the policy monitor question to the Magistrate component.
Vulnerability Score Adjustments	Adjusts the vulnerability risk score of an asset, depending if the question fails or passes. The vulnerability risk scores are adjusted in IBM Security QRadar Vulnerability Manager.

Additional Actions	The additional actions to be taken when an event is received.
	
	Separate multiple email addresses using a comma.
	
	Select **Notify** if you want events that generate as a result of this monitored question to display events in the System Notifications item in the dashboard.
	
	The syslog output might resemble:
	
	`Sep 28 12:39:01 localhost.localdomain ECS:`
	`Rule 'Name of Rule'`
	`Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6,`
	`Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011,`
	` Notes: Event description`

Enable Monitor	Monitor the question.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question you want to monitor.
4. Click **Monitor**.
5. Configure values for the parameters.
6. Click **Save Monitor**.

Group questions

You can group and view your questions based on your chosen criteria

Categorizing your questions allows you to efficiently view and track your questions. For example, you can view all questions related to compliance.

As you create new questions, you can assign the question to an existing group.

Viewing groups

You can view a group of your questions.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Group** list, select the group you want to view.

Creating a group

You can create a new group for questions.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Click **Groups**.
4. From the menu tree, select the group under which you want to create a new group.
5. Click **New**.
6. In the **Name field,** specify the name that you want to assign to the new group. The name can be up to 255 characters in length.
7. In the **Description field,** specify a description that you want to assign to this group. The description can be up to 255 characters in length.
8. Click **OK**.
9. If you want to change the location of the new group, click the new group and drag the folder to the chosen location in your menu tree.

Editing a group

You can edit a group of questions.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.

3. Click **Groups**.
4. From the menu tree, select the group you want to edit.
5. Click **Edit**.
6. Edit the **Name** and **Description**, as required.

   The name and description fields can be a maximum of 255 characters.
7. Click **OK**.
8. If you want to change the location of the group, select the group and drag the folder to the preferred location in the menu tree.
9. Close the Groups window.

Copying an item to another group

Using the groups functionality, you can copy a simulation to one or many groups.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the question you want to copy to another group.
5. Click **Copy**.
6. Select the check box for the group to which you want to copy the simulation.
7. Click **Copy**.

Deleting an item from a group

You can delete an item from a group.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the top level group.
5. From the list of groups, select the item or group you want to delete.
6. Click **Remove**.
7. Click **OK**.

Assigning an item to a group

You can assign a question to a group.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. Select the question you want to assign to a group.
4. Using the **Actions** menu, select **Assign Groups**.
5. Select the group to which you want the question assigned.
6. Click **Assign Groups**.

QRadar Risk Manager and QRadar Vulnerability Manager integration

IBM Security QRadar Vulnerability Manager integrates with IBM Security QRadar Risk Manager to help you prioritize the risks and vulnerabilities in your network.

Risk policies and vulnerability prioritization

You can integrate QRadar Vulnerability Manager with QRadar Risk Manager by defining and monitoring asset or vulnerability risk policies.

When the risk policies that you define in QRadar Risk Manager either pass or fail, vulnerability risk scores in QRadar Vulnerability Manager are adjusted. The adjustment levels depend on the risk policies in your organization.

When the vulnerability risk scores are adjusted in QRadar Vulnerability Manager, administrators can do the following tasks:

- Gain immediate visibility of the vulnerabilities that failed a risk policy.

  For example, new information might be displayed on the QRadar dashboard or sent by email.
- Re-prioritize the vulnerabilities that require immediate attention.

  For example, an administrator can use the **Risk Score** to quickly identify high-risk vulnerabilities.

If you apply risk policies at an asset level in QRadar Risk Manager, then all the vulnerabilities on that asset have their risk scores adjusted.

Policy Monitor use cases

Many options are available when you create questions to analyze your network for risk.

The following Policy Monitor examples outline common use cases that you can use in your network environment.

Asset test for possible communication on protected assets

This use case demonstrates how to create a Policy Monitor question based on IP address. All organizations have networks that contain critical servers where traffic is monitored and only accessible by trusted employees.

About this task

From a risk perspective, it is important to know which users within your organization can communicate with critical network assets. IBM Security QRadar Risk Manager accomplishes this task by creating a Policy Monitor question based on an asset test for possible communications.

There are several ways a Policy Monitor question can be generated for this use case objective. You could look at all the connections to the critical server over time, but you might be more concerned that regional employees are not accessing these critical servers. To accomplish this, you can create a Policy Monitor question that looks at the topology of the network by IP address.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New**.
4. In the **What do you want to name this question field,** type a name for the question.
5. In the **What type of data do you want to return drop-down list, select Assets**.
6. From the **Evaluate On drop-down list, select Possible Communication**.
7. From the **Importance Factor drop-down list,** specify a level of importance to associate with your question.
8. In the **Time Range section, specify** a time range for the question.
9. In the **Which tests do you want to include in your question** section, double-click to select **have accepted communication to destination asset building blocks**.
10. In the Find Assets that section, click **asset building blocks** to further configure this test and specify **Protected Assets**.

    Note: To define your network remote assets, you must have previously defined your remote assets building block.
11. In the **Which tests do you want to include in your question** section, double-click to select the restrictive test **and include only the following IP addresses**.
12. In the Find Assets that section, click **IP Addresses**.
13. Specify the IP address range or CIDR address of your remote network.
14. Click **Save Question**.
15. Select the Policy Monitor question you created for protected assets.
16. Click **Submit Question**.
17. Review the results to see if any protected asset has accepted communication from an unknown IP address or CIDR range.
18. Optional. After the results have been properly tuned you can monitor your protected assets by putting the question into monitoring mode. If an unrecognized IP address connects to a protected asset, then QRadar Risk Manager can generate an alert.

What to do next

You can monitor your questions.

Device/Rule test communication on Internet access

This use case demonstrates how to create a Policy Monitor question based on devices/rules. Device tests identify rules in a device that violate a defined policy or changes that introduced risk into the environment.

About this task

Device tests identify rules in a device that violate a defined policy or changes that introduced risk into the environment. From a network perspective, it is important to know which device rules could have changed and alert you to the rule so it can be corrected. A very common occurrence is when servers that did not previously have Internet access are granted access due to a firewall change on the network.

IBM Security QRadar Risk Manager can monitor for rule changes on network devices by creating a Policy Monitor question based on the device rules.

There are several ways a Policy Monitor question can be generated for this use case objective. In this example, you will create a Policy Monitor question that looks to see what devices have access to the internet.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New**.
4. In the **What type of data do you want to return drop-down list, select Devices/Rules**.
5. From the **Importance Factor drop-down list,** specify a level of importance to associate with your question.
6. In the **Which tests do you want to include in your question** section, double-click to select **allow connection to the internet**.
7. Click **Save Question**.
8. Select the Policy Monitor question you created for monitoring device rules.
9. Click **Submit Question**.
10. Review the results to see if any rules allow access to the internet.
11. Optional. After the results have been properly tuned you can monitor your protected assets by putting the question into monitoring mode.

What to do next

You can monitor your questions.

Prioritizing high risk vulnerabilities by applying risk policies

In IBM Security QRadar Vulnerability Manager, you can alert administrators to higher risk vulnerabilities by applying risk policies to your vulnerabilities.

When you apply a risk policy, the risk score of a vulnerability is adjusted, allowing administrators to prioritize more accurately the vulnerabilities that require immediate attention.

In this example, the vulnerability risk score is automatically increased by a percentage factor for any vulnerability that remains active on your network after 40 days.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Manage Vulnerabilities**.
3. On the toolbar click **Search** > **New Search**.
4. In the Search Parameters pane, configure the following filters:
   a. **Risk Equals High**
   b. **Days since vulnerabilities discovered Greater than or equal to 40**
5. Click **Search** and then on the toolbar click **Save Search Criteria**.

   Type a saved search name that is identifiable in QRadar Risk Manager.
6. Click the **Risks** tab.

7. In the navigation pane, click **Policy Monitor**.

8. On the toolbar click **Actions** > **New**.

9. In the **What do you want to name this question** field, type a name.

10. In the **Which tests do you want to include in your question** field, click **are susceptible to vulnerabilities contained in vulnerability saved searches**.

11. In the **Find Assets that** field, click the underlined parameter on the **are susceptible to vulnerabilities contained in vulnerability saved searches**.

12. Identify your QRadar Vulnerability Manager high risk vulnerability saved search, click **Add**, then click **OK**.

13. Click **Save Question**.

14. In the Questions pane, select your question from the list and on the toolbar click **Monitor**.

   Restriction: The **Event Description** field is mandatory.

15. Click **Dispatch question passed events**.

16. In the **Vulnerability Score Adjustments** field, type a risk adjustment percentage value in the **Percentage vulnerability score adjustment on question fail** field.

17. Click **Apply adjustment to all vulnerabilities on an asset** then click **Save Monitor**.

What to do next

On the **Vulnerabilities** tab, you can search your high risk vulnerabilities and prioritize your vulnerabilities

Actual communication for DMZ allowed protocols

This use case demonstrates how to create a Policy Monitor question based on the known list of trusted protocols for the DMZ. In most organizations, network traffic crossing the DMZ is restricted to well known and trusted protocols, such as HTTP or HTTPS on specified ports.

About this task

From a risk perspective, it is important to continuously monitor traffic in the DMZ to ensure that only trusted protocols are present. IBM Security QRadar Risk Manager accomplishes this by creating a Policy Monitor question based on an asset test for actual communications.

There are several ways a Policy Monitor question can be generated for this use case objective. Since we know network policy only allows a few trusted protocols, we select an option to create our Policy Monitor question based on the known list of trusted protocols for the DMZ.

Procedure

1. Click the **Risks** tab.

2. On the navigation menu, click **Policy Monitor**.

3. From the **Actions** menu, select **New**.

4. In the **What do you want to name this question field,** type a name for the question.

5. In the **What type of data do you want to return drop-down list, select Assets**.

6. From the **Evaluate On drop-down list, select Actual Communication.**
7. From the **Importance Factor drop-down list,** specify a level of importance to associate with your question.
8. In the **Time Range section, specify** a time range for the question.
9. In the **Which tests do you want to include in your question** section, select **have accepted communication to destination networks**.
10. In the **Find Assets that** section, click **destination networks** to further configure this test and specify your DMZ as the destination network.
11. Select the **and include the following inbound ports**.
12. In the **Find Assets that** section, click the include only parameter so that it changes to exclude. The parameter now displays and exclude the following inbound ports.
13. Click **ports**.
14. Add port 80 and 443, and then click **OK**.
15. Click **Save Question**.
16. Select the Policy Monitor DMZ question you created.
17. Click **Submit Question**.
18. Review the results to see if any protocols other than port 80 and port 443 are communicating on the network.
19. Optional. After the results have been properly tuned, you can monitor your DMZ question by putting the question into monitoring mode

What to do next

You can monitor your questions.

CIS benchmark scans

To set up a CIS benchmark scan, you must carry out a range of configuration tasks on the Admin, Assets, Vulnerabilities, and Risks tabs in QRadar.

In order to set up CIS benchmark scan, the following prerequisites are needed:

Valid IBM Security QRadar Vulnerability Manager and IBM Security QRadar Risk Manager licenses

If you patched from an earlier version of IBM Security QRadar, you must do an automatic update before you do a CIS benchmark scan.

There are 8 steps involved in setting up a CIS benchmark scan:
1. Adding assets.
2. Configuring a credential set.

   It is easiest to add centralized credentials on the IBM Security QRadar Admin tab but you can also add credentials when you create a benchmark profile.
3. Creating an asset saved search.

   You use the asset saved searches when you configure the asset compliance questions.
4. Modifying CIS benchmark checks in QRadar Vulnerability Manager.

   You can create a custom CIS benchmark checklist by using the Compliance Benchmark Editor.
5. Configuring a CIS benchmark scan profile in QRadar Vulnerability Manager.

6. Creating an asset compliance question in IBM Security QRadar Risk Manager.

7. Monitoring the asset compliance question that you created.

8. Viewing the CIS benchmark scan results.

Adding or editing an asset profile

Before you can do a CIS benchmark scan you must add the network assets you intend to scan to IBM Security QRadar. Asset profiles are automatically discovered and added; however, you might be required to manually add a profile.

About this task

You can enter information on each asset manually by creating an Asset Profile on the **Assets** tab. Alternatively, you can configure a scan profile on the **Vulnerabilities** tab to run a discovery scan. The discovery scan allows QRadar® to identify key asset characteristics such as operating system, device type, and services.

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

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

Procedure

1. Click the **Assets** tab.

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

3. Choose one of the following options:

   To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.

   To edit an asset, double-click the asset that you want to view and click **Edit Asset** .

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

   Click the **New MAC Address** icon and type a MAC Address in the dialog box.

   Click the **New IP Address** icon and type an IP address in the dialog box.

   If **Unknown NIC** is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.

   Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.

   Select a MAC or IP address from the list and click the **Remove** icon.

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

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

6. Configure the parameters in the Operating System pane:
   a. From the **Vendor** list box, select an operating system vendor.
   b. From the **Product** list box, select the operating system for the asset profile.
   c. From the **Version** list box, select the version for the selected operating system.
   d. Click the **Add** icon.
   e. From the **Override** list box, select one of the following options:
      • **Until Next Scan** - Select this option to specify that the scanner provides operating system information and the information can be temporarily edited. If you edit the operating system parameters, the scanner restores the information at its next scan.
      • **Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.
   f. Select an operating system from the list.
   g. Select an operating system and click the **Toggle Override** icon.
7. Configure the parameters in the CVSS & Weight pane. Configure one or more of the following options:

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

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

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

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

Parameter	Description
Technical Owner	Type the technical owner of the asset. An example of a business owner is the IT manager or director. The maximum length is 255 characters.
Technical Owner Contact	Type the contact information for the technical owner. The maximum length is 255 characters.
Technical User	From the list box, select the username that you want to associate with this asset profile. You can also use this parameter to enable automatic vulnerability remediation for IBM Security QRadar Vulnerability Manager. For more information about automatic remediation, see the *IBM Security QRadar Vulnerability Manager User Guide*.

9. Click **Save**.

Configuring a credential set

In IBM Security QRadar Vulnerability Manager, you can create a credential set for the assets in your network. During a scan, if a scan tool requires the credentials for a Linux, UNIX, or Windows operating system, the credentials are automatically passed to the scan tool from the credential set.

Procedure

1. Click the **Admin** tab.
2. In the **System Configuration** pane, click **Centralized Credentials**.
3. In the Centralized Credentials window, on the toolbar, click **Add**.

   To configure a credential set, the only mandatory field in the Credential Set window is the **Name** field.
4. In the Credential Set window, click the **Assets** tab.
5. Type a CIDR range for the assets that you want to specify credentials for and click **Add**.

   Users must have network access permissions that are granted in their security profile for an IP address or CIDR address range that they use or create credentials for in **Centralized Credentials**.
6. Optional: Click the **Linux/Unix, Windows, or Network Devices (SNMP)** tabs, then type your credentials.
7. Click **Save**.

Saving asset search criteria

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

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Perform a search.
4. Click **Save Criteria** .
5. Enter values for the parameters:

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

Editing a compliance benchmark

Use the Compliance Benchmark Editor in IBM Security QRadar Risk Manager to add or remove tests from the default CIS benchmarks.

Procedure

1. Click the **Risks** tab.
2. Click **Policy Monitor**.
3. Click **Compliance** to open the Compliance Benchmark Editor window.
4. On the navigation menu, click the default CIS benchmark that you want to edit.
5. In the **Compliance** pane, click the **Enabled** check box in the row that is assigned to the test that you want to include.

   Click anywhere on a row to see a description of the benchmark test, a deployment rationale, and information on things to check before you enable the test.

   When you are building a custom CIS checklist, be aware that some benchmark tests that are not included by default can take a long time to run. For more information, please refer to the CIS documentation.

What to do next

Create an asset compliance question to test assets against the benchmark you edited.

Related tasks:

"Creating an asset compliance question" on page 41
Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Creating a benchmark profile

To create Center for Internet Security compliance scans, you must configure benchmark profiles. You use CIS compliance scans to test for Windows and Red Hat Enterprise Linux CIS benchmark compliance.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Administrative** > **Scan Profiles**.
3. On the toolbar, click **Add Benchmark**.
4. If you want to use pre-defined centralized credentials, select the **Use Centralized Credentials** check box.

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
5. If you are not using dynamic scanning, select a QRadar Vulnerability Manager scanner from the **Scan Server** list.
6. To enable dynamic scanning, click the **Dynamic server selection** check box.

   If you configured domains in the **Admin** > **Domain Management** window, you can select a domain from the **Domain** list. Only assets within the CIDR ranges and domains that are configured for your scanners are scanned.
7. In the **When To Scan** tab, set the run schedule, scan start time, and any pre-defined operational windows.
8. In the **Email** tab, define what information to send about this scan and to whom to send it.
9. If you are not using centralized credentials, add the credentials that the scan requires in the **Additional Credentials** tab.

   Credentials that are used to scan Linux operating systems must have root privileges. Credentials that are used to scan Windows operating systems must have administrator privileges.
10. Click **Save**.

Creating an asset compliance question

Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Before you begin

Policy Monitor questions are evaluated in a top down manner. The order of Policy Monitor questions impacts the results.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. From the **Actions** menu, select **New Asset Compliance Question**.
4. In the **What do you want to name this question** field, type a name for the question.
5. Select the level of importance you want to associate with this question from the **Importance Factor** list.
6. From the **Which tests do you want to include in your question** field, select the add (+) icon beside the **test compliance of assets in asset saved searches with CIS benchmarks** test.

   Select this test multiple times, if necessary.
7. Configure the parameters for your tests in the **Find Assets that** field.

   Click each parameter to view the available options for your question. Specify multiple assets saved searches and multiple checklists in this test, if necessary.

8. In the group area, click the relevant check boxes to assign group membership to this question.

   Asset compliance questions must be assigned to a group for inclusion in compliance dashboards or reports.

9. Click **Save Question**.

What to do next

Associate a benchmark profile with, and monitor the results of, the question you created.

Related concepts:

"Importance factor" on page 38
The Importance Factor is used to calculate the Risk Score and define the number of results returned for a question.

"Group questions" on page 53
You can group and view your questions based on your chosen criteria

Related tasks:

"Monitoring asset compliance questions" on page 43
Monitor asset compliance questions by selecting CIS scan profiles. CIS benchmark scans run against the assets.

Monitoring asset compliance questions

Monitor asset compliance questions by selecting CIS scan profiles. CIS benchmark scans run against the assets.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Policy Monitor**.
3. In the **Questions** pane, select the asset compliance question that you want to monitor.
4. Click **Monitor** to open the Monitor Results window.
5. Select a benchmark profile from the **Which benchmark profile to associate with this question?** list.

   The selected benchmark scan profile uses a QRadar Vulnerability Manager scanner that is associated with a domain. The domain name is displayed in the **Benchmark Profile Details** area. For more information about domain management, see the *IBM Security QRadar SIEM Administration Guide*.
6. Select the **Enable the monitor results function for this question/simulation** check box.
7. Click **Save Monitor**.

   Monitoring begins at the scan start time that you set on the **When To Scan** tab when you created the benchmark scan profile.

Related tasks:

"Editing a compliance benchmark" on page 42
Use the Compliance Benchmark Editor in IBM Security QRadar Risk Manager to add or remove tests from the default CIS benchmarks.

"Creating an asset compliance question" on page 41
Create an asset compliance question in Policy Monitor to search for assets in the network that fail CIS benchmark tests.

Viewing scan results

The Scan Results page displays a summary list of the results generated by running a scan profile.

About this task

The Scan Results page provides the following information:

Table 12. Scan results list parameters

Parameter	Description
Profile	The name of the scan profile. Hover your mouse over the **Profile** to display information about the scan profile and the status of the scan.
Schedule	The run schedule that is applied to the scan profile. If you initiated a manual scan then **Manual** is displayed.
Score	The average Common Vulnerability Scoring System (CVSS) score for the scan. This score helps you prioritize vulnerabilities.
Hosts	The number of hosts found and scanned when the scan profile ran. Click the **Host** column link to display vulnerability data for the scanned hosts.
Vulnerabilities	The number of different types of vulnerabilities found by a scan. Click the **Vulnerabilities** column link to view all unique vulnerabilities.
Vulnerability Instances	The number of vulnerabilities found by the scan.
Open Services	The number of unique open services found by the scan. A unique open service is counted as a single open service. Click the **Open Services** column link to view vulnerabilities categorized by open service.
Status	The status of the Scan Profile, options include: Stopped - This status is displayed if the scan completed successfully or the scan was canceled. Running - The scan is running Paused - The scan is paused. Not Started - The scan is not initiated.
Progress	Specifies the progress of the scan. Hover your mouse over the progress bar, while the scan is running, to display information about the status of a scan.
Start Date/Time	The date and time when the scan profile started running.
Duration	Displays the time taken for the scan to complete.

Procedure

1. Click the **Vulnerabilities** tab.
2. In the navigation pane, click **Scan Results**.

Monitoring firewall rule event counts of Check Point devices

In IBM Security QRadar Risk Manager, you can monitor the firewall rule event counts of your Check Point devices by integrating with the Check Point SMS. You can view these rule interactions in QRadar Risk Manager, and use rule reports to manage the rule policy effectiveness of your network.

In the following image, QRadar receives and processes rule event logs from Check Point firewall devices through the SMS.
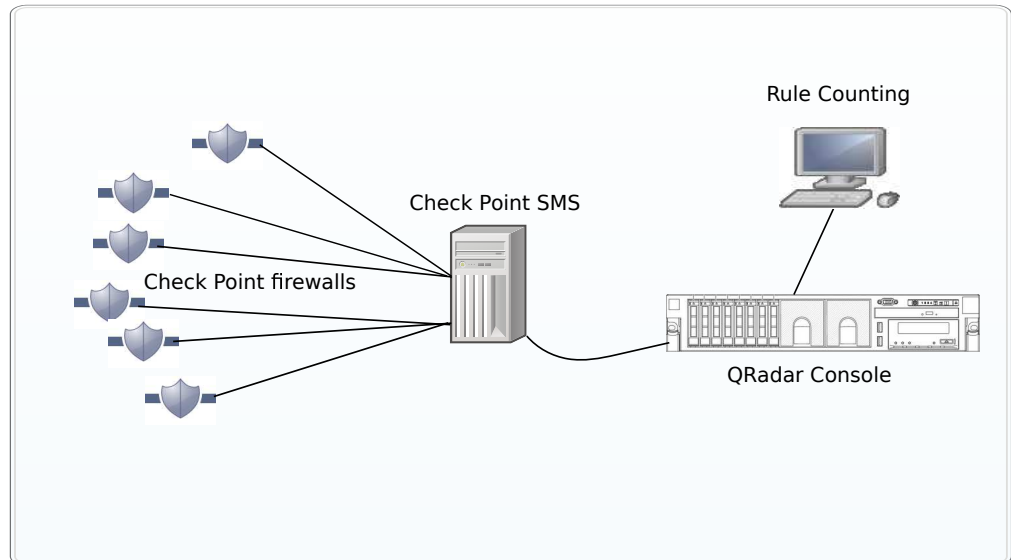
Figure 1. Check Point rule counting

Scenario - Implementing Check Point firewall rule monitoring in QRadar

You are a network systems administrator with responsibility for Network security in an organization that uses Check Point to implement its Network security policies. The network includes several Check Point firewalls that are managed from a Check Point Security Management Server (SMS).

You want to view reports on rule usage daily, so that you have more visibility on your rule implementation.

You need to configure a connection between your Check Point SMS and QRadar, so that QRadar receives rule event logs from Check Point firewall devices. QRadar processes this rule event log information and displays rule event information for all devices that are managed by Check Point firewalls. From the QRadar rules table, you can analyze the usage and effectiveness of the firewall rules by monitoring event counts, and fine-tune your rules for optimal performance.

Use the rule information to do the following tasks:

- View most and least used rules.
- Assess the practicality of rules that are triggered infrequently.

- View rules that might be blocking network access unnecessarily.
- View rules that are triggered excessively, and place a load on your network bandwidth.
- View detailed events.
- Schedule reports.

Before you begin, download the most recent adapter bundle from FixCentral, and install it on your QRadar managed host.

Complete the following steps to set up rule counting:

1. Configure OPSEC applications in the Check Point SmartDashboard.
2. Create a log source in QRadar.
3. Configure Configuration Source Management (CSM) in QRadar Risk Manager. Discover and backup devices in Configuration Source Management.
4. Complete the configurations to view rule counting.

Configuring OPSEC applications in the SmartDashboard

Create and configure 2 OPSEC applications in your Check Point SmartDashboard. This facilitates the transfer of log files between Check Point and IBM Security QRadar.

About this task

Create 2 OPSEC (Open Platform for Security) applications, one with a client entity property of CPMI (Check Point Management Interface) for QRadar Risk Manager, and the other with a client entity property of LEA (Log Export API) for the QRadar Risk Manager log source.

Procedure

1. From the **Manage** menu on the toolbar, click **Servers and OPSEC Applications**.
2. Click **New** > **OPSEC Application**.
3. In the **Name** field, type a name for the application.
4. From the **Host** list, select a host, or click **New** to add a host.
5. Under **Client Entities**, select the **CPMI** check box.

   This option is required for QRadar Risk Manager Configuration Source Management (CSM).
6. Click **Communication**.
7. In the **One-time password** field, type a password and then confirm it.

   The password is used several times during setup, and you need to reuse it so that QRadar can use a security certificate from Check Point.
8. Click `Initalize`.

   The **Trust state** changes to: `Initialized but trust not established`.
9. Click **Close**.
10. To populate the **DN** field in the Secure Internal Communication section, click **OK**.
11. To view the populated **DN** field, select your OPSEC Application, and click **Edit**

    The **DN** field is now populated. This information is used for the **Application Object SIC Attribute (SIC Name)** and the **SIC Attribute (SIC Name)** when you set up the log source and Configuration Source Management in QRadar

12. Create the second OPSEC application to use with the log source.

Follow steps 1-11 for creating the first OPSEC Application, with two exceptions:

- For the **Name** field in step 3, use a different name from the first OPSEC application.
- For **Client Entities** in step 5, select the **LEA** check box.

Make sure that the **Trust state** displays `Initialized but trust not established`.

Tip: Use the same one-time password for this OPSEC application to avoid any confusion with passwords.

13. In SmartDashboard, close all windows until you get back to the main SmartDashboard window.
14. From the **Policy** menu on the toolbar, click **Install**.
15. Click **Install on all selected gateways, if it fails do not install on gateways of the same version**.

What to do next

The next step is to configure the log source in QRadar.

Configuring the log source

Configure the log source in IBM Security QRadar to get a certificate from Check Point and to receive log information.

Procedure

1. Log on to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.

   The Data Sources pane is displayed.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. Configure the following values:

Table 13. Check Point log source parameters

Parameter	Description
Log Source Name	The identifier for the log source.
Log Source Description	The description is optional.
Log Source Type	Select **Check Point FireWall-1**.
Protocol Configuration	Select **OPSEC/LEA**.
Log Source Identifier	IP address of your SMS
Server IP	Type the IP address of your SMS
Server Port	Use port 18184.
Use Server IP for Log Source	Do not select this check box.
Statistics Report Interval	Default of 600.
Authentication Type	From the list, select **sslca**.

Table 13. Check Point log source parameters (continued)

Parameter	Description
OPSEC Application Object SIC Attribute (SIC Name)	From the Check Point SmartDashboard, click **Manage** > **Servers and OPSEC Applications** and select the OPSEC application that has the client entity property of LEA. Click **Edit**, and copy the entry from the **DN** field, and paste into the **OPSEC Application Object SIC Attribute (SIC Name)** field.

Log Source SIC Attribute (Entity SIC Name)	Use the entry that you pasted into the **OPSEC Application Object SIC Attribute (SIC Name)** field, remove the text from the `CN=` property value, and make the following edits:
	
	For the `CN=` property value, use `cp_mgmt_` *<hostname >*
	
	where *<hostname>* is the **Host** name from the OPSEC Application Properties window.
	
	See the following examples of an OPSEC Application DN and OPSEC Application Host, which is used to create the Entity SIC Name:
	
	OPSEC Application DN: `CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx`
	
	OPSEC Application Host: `Srvxxx-SMS`
	
	Use text from the OPSEC Application DN and the OPSEC Application Host to form the **Entity SIC Name**:
	
	`CN=cp_mgmt_Srvxxx-SMS,O=svxxx-CPSMS..bsaobx`
	
	The **Entity SIC Name** in this configuration is based on a Gateway to Management Server setup. If your SMS address is not used as a gateway, use the Management Server configuration for the **Entity SIC Name,** which is represented by the following text:
	
	`CN=cp_mgmt,O=<take_O_value_from_DN_field>`

Specify Certificate	Don't select this check box.
Certificate Authority IP	Type the IP address of the SMS.
Pull Certificate Password	The password that you specified for the OPSEC Applications Properties in the **One-time password** field of the Communication window.
OPSEC Application	The name that you specified in the **Name** field from the OPSEC Applications Properties.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases when multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.

Table 13. Check Point log source parameters (continued)

Parameter	Description
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings properties in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings properties in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

7. Click **Save**.
8. On the **Admin** tab, click **Deploy Changes**.

   If you find that changes are implemented automatically, it's still good practice to click **Deploy Changes**.

   Check that trust is established for the OPSEC application that has the client entity property of LEA, by viewing the **Trust State** in the Communication window of OPSEC Application Properties.

   The configuration of the log source is complete.

   For more information about configuring log sources, see the *IBM Security QRadar Managing Log Sources Guide*.

Establishing secure communication between Check Point and IBM Security QRadar

Configure Configuration Source Management in IBM Security QRadar to connect to the Check Point SMS. Add the OPSEC Application details from the SmartDashboard, and request a security certificate from Check Point.

About this task

Configure the OPSEC application details in Configuration Source Management and set up the certificate exchange. After the configuration is complete, use Configuration Source Management to discover the new entry.

Procedure

1. Log in to QRadar as an administrator.
2. Click the **Admin** tab.
3. On the navigation menu, click **Plug-ins** or scroll down to find the **Configuration Source Management** icon.
4. Click the **Configuration Source Management** icon.
5. On the navigation menu, click **Credentials**.
6. From the Network Groups pane, click the **(+)** symbol.
7. Type a name for the network group.
8. In the **Add address (IP, CIDR, Wildcard, or Range)** field, type the IP address of your SMS.
9. Click **(+)** to add the IP address.
10. Type your SMS SmartDashboard user name and password.

To configure the OPSEC fields, use the information from the OPSEC Application Properties window of the SmartDashboard, where you selected the **CPMI** check box for the client entity.

11. From the **DN** field, copy and paste this information into the **OPSEC Entity SIC Name** field.

12. Edit the entry that you pasted into the **OPSEC Entity SIC Name** by replacing the CN= property value with: cp_mgmt_<*hostname*>

    where <*hostname*> is the **Host** name that is used for the OPSEC application **Host** field.

    See the following examples of an OPSEC Application DN and OPSEC Application Host, which is used to create the Entity SIC Name:
    • OPSEC Application DN: `CN=cpsmsxxx,O=svxxx-CPSMS..bsaobx`
    • OPSEC Application Host: `Srvxxx-SMS`

    Use text from the OPSEC Application DN and the OPSEC Application Host to form the **Entity SIC Name**:

    The **Entity SIC Name** is `CN=cp_mgmt_Srvxxx-SMS,O=svxxx-CPSMS..bsaobx`

    The **Entity SIC Name** in this configuration is based on a Gateway to Management Server setup. If your SMS IP address in not used as a gateway, use the Management Server configuration from the table:

Table 14. Entity SIC Name formats

Type	Name
Management Server	`CN=cp_mgmt,O=<take_O_value_from_DN_field>`
Gateway to Management Server	`CN=cp_mgmt_<gateway_hostname>,O=<take_O_value from_DN_field>`

13. From the **DN** field, copy the entry, and paste this information into the **OPSEC Application Object SIC Name** field.

14. Click **Get Certificate**.

15. Enter the SMS IP address in the **Certificate Authority IP** field.

16. Enter the one-time password in the **Pull Certificate Password** field. The one-time password is from the Communication window in the OPSEC Application Properties of the SmartDashboard, where you selected the **CPMI** check box for the client entity.

17. Click **OK**

    If successful, the **OPSEC SSL Certificate** field is populated and grayed out.

    Verify that the **Trust State** property in the Communication window of the OPSEC Application Properties changes to `Trust established`.

    The credentials are set up, and now you can run a discovery.

18. On the navigation menu, click **Discover From Check Point SMS**.

19. In the **CPSMS IP Address** field, type the IP address of the SMS.

Initializing rule counting for Check Point

Complete the final configurations in IBM Security QRadar and Check Point to tie the configurations together so that you can use rule counting in QRadar.

About this task

When trust is established and the policies are updated, you can view rule counting in QRadar. QRadar Risk Manager needs approximately 1 hour to process counts.

Procedure

1. In QRadar, click **Risks** > **Configuration Monitor**
2. Double-click a Check Point device to view the rule counting.
   - Verify that the log source is auto mapping by looking in the **Log Sources** column.
   - Look for the **Event Count** column of the rules table.

Policy Monitor questions

You can define test questions to identify risk in network devices or rules on network devices.

Generic and test-specific parameters for Policy Monitor tests

You configure parameters for each Policy Monitor test. Configurable parameters are bolded and underlined. You click a parameter to view the available options for your question.

Policy Monitor tests use two types of parameters; generic and test-specific. Generic parameters provide 2 or more options to customize a test. Clicking a generic parameter toggles the choices that are available. Test-specific parameters require user-input. You click test-specific parameters to specify information.

For example, the asset test called **have accepted communication to destination remote network locations** contains two generic parameters and one test-specific parameter. Click the generic parameter, **have accepted**, to select either **have accepted** or **have rejected**. Click the generic parameter, **to destination**, to select either **to destination** or **from source**. Click the test-specific parameter, **remote network locations**, to add a remote location for the asset test.

Asset test questions

Asset questions are used to identify assets on the network that violate a defined policy or introduce risk into the environment.

Asset test questions are categorized by communication type; actual or possible. Both communication types use contributing and restrictive tests.

Actual communication includes any assets on which communications have been detected using connections. Possible communication questions allow you to review if specific communications are possible on assets, regardless of whether or not a communication has been detected.

A contributing test question is the base test question that defines what type of actual communication you are trying to test.

A restrictive test question restricts the test results from the contributing test to further filter the actual communication for specific violations.

When you use a restrictive test, the direction of the restrictive test should follow the same direction as the contributing test. Restrictive tests that use a mix of inbound and outbound directions can be used in situations where you are trying to locate assets in between two points, such as two networks or IP addresses.

Inbound refers to a test that is filtering the connections for which the asset in question is a destination. Outbound refers to a test that is filtering connections for which the asset in question is a source.

Devices/Rules test questions

Devices and rules are used to identify rules in a device that violate a defined policy that can introduce risk into the environment.

For a detailed list of device rule questions, see Device/rules test questions.

Contributing questions for actual communication tests

The actual communication tests for assets include contributing questions and parameters that you choose when you create a policy monitor test.

When you apply the have not condition to a test, the not condition is associated with the parameter that you are testing.

For example, if you configure a test as **have not accepted communication to destination networks**, then the test detects assets that have accepted communications to networks other than the configured network. Another example is if you configure a test as have not accepted communication to the Internet, then the test detects assets that have accepted communications from or to areas other than the Internet.

The following table lists and describes the contributing question parameters for actual communication tests.

Table 15. Contributing question parameters for actual communication tests

Test Name	Description
have accepted communication to any destination	Detects assets that have communications to any or from any configured network. This test allows you to define a start or end point to your question. For example, to identify the assets that have accepted communication from the DMZ, configure the test as follows: have accepted communication from any source You can use this test to detect out-of-policy communications.

Test Name	Description
have accepted communication to destination networks	Detects assets that have communications to or from the networks that you specify. This test allows you to define a start or end point to your question. For example, to identify the assets that communicated to the DMZ, configure the test as follows: have accepted communication from source <networks> You can use this test to detect out-of-policy communications.
have accepted communication to destination IP addresses	Detects assets that have communications to or from the IP address that you specify. This test allows you to specify IP or CIDR address. For example, if you want to identify all assets that communicated to a specific compliance server, configure the test as follows: have accepted communications to destination <compliance server IP address>
have accepted communication to destination asset building blocks	Detects assets that have communications to or from the asset building blocks that you specify. This test allows you to re-use building blocks defined in the QRadar Rules Wizard in your query. For more information about rules, assets, and building blocks, see the *IBM Security QRadar SIEM Administration Guide*.
have accepted communication to destination asset saved searches	Detects assets that have communications to or from the assets that are returned by the saved search that you specify. For information about creating and saving an asset search, see the *IBM Security QRadar SIEM Users Guide*
have accepted communication to destination reference sets	Detects assets that have communicated to or from the defined reference sets.
have accepted communication to destination remote network locations	Detects assets that have communicated with networks defined as a remote network. For example, this test can identify hosts that have communicated to botnets or other suspicious Internet address space.

Table 15. Contributing question parameters for actual communication tests (continued)

Test Name	Description
have accepted communication to destination geographic network locations	Detects assets that have communicated with networks defined as geographic networks. For example, this test can detect assets that have attempted communications with countries in which you do not have business operations.
have accepted communication to the Internet	Detects source or destination communications to or from the Internet.
are susceptible to one of the following vulnerabilities	Detects specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the test, **are susceptible to vulnerabilities with one of the following classifications**. You can search for vulnerabilities by using the OSVDB ID, CVE ID, Bugtraq ID, or title.
are susceptible to vulnerabilities with one of the following classifications	A vulnerability can be associated with one or more vulnerability classifications. This test filters all assets that include vulnerabilities with the specified classifications. Configure the **classifications** parameter to identify the vulnerability classifications that you want this test to apply. For example, a vulnerability classification might be Input Manipulation or Denial of Service.
are susceptible to vulnerabilities with CVSS score greater than 5	A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of vulnerabilities. CVSS is composed of 3 metric groups: Base, Temporal, and Environmental. These metrics allow CVSS to define and communicate the fundamental characteristics of a vulnerability. This test filters assets in your network that include vulnerabilities with the CVSS score that you specify.
are susceptible to vulnerabilities disclosed after specified date	Detects assets in your network with a vulnerability that is disclosed after, before, or on the configured date.
are susceptible to vulnerabilities on one of the following ports	Detects assets in your network with a vulnerability that is associated with the configured ports. Configure the **ports** parameter to identify ports you want this test to consider.

Table 15. Contributing question parameters for actual communication tests (continued)

Test Name	Description
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more text entry. Configure the **text entries** parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression. Configure the **regular expressions** parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in IBM Security QRadar Vulnerability Manager.

Deprecated contributing test questions

Contributing questions that are replaced by another test are hidden in policy monitor.

The following tests are hidden in the Policy Monitor:
- assets that are susceptible to vulnerabilities
- assets that are susceptible to vulnerabilities from the following services

These contributing tests have been replaced by other tests.

Restrictive questions for actual communication tests

The actual communication tests for assets include restrictive questions and parameters that you can choose when you create a policy monitor test.

When you apply the exclude condition to a test, the exclude condition applies to the protocols parameter.

For example, if you configure this test to **exclude the following protocols**, the test will return only assets that do not use the excluded protocols.

The following table lists and describes the restrictive question parameters for actual communication tests.

Table 16. Restrictive question parameters for actual communication tests

Test Name	Description
include only the following protocols	Filters assets from the contributing test that include or exclude the specified protocols. This test is only selectable when a contributing asset test is added to this question.

Table 16. Restrictive question parameters for actual communication tests (continued)

Test Name	Description
include only the following inbound ports	Filters assets from the contributing test that include only or exclude the specified ports.

This test is only selectable when a contributing asset test is added to this question. |
| include only the following inbound applications | Filters assets from the contributing test question that include only or exclude any inbound or outbound applications.

This test filters connections that only include flow data. |
| include only if the source inbound and destination outbound bytes have a percentage difference less than 10 | Filters assets from the contributing test question that is based on communications with a specific ratio of inbound to outbound (or outbound to inbound) bytes.

This test is useful for detecting hosts that might be exhibiting proxy type behavior (inbound equals outbound). |
| include only if the inbound and outbound flow count has a percentage difference less than 10 | Filters assets from the contributing test question that is based on communications with a specific ratio of inbound to outbound (or outbound to inbound) flows.

This test filters connections that include flow data when flow count is selected.

This restrictive test requires two contributing tests that specify a source and destination. The following test outlines a set of questions trying to determine what assets between two points have an inbound and outbound percentage difference greater than 40%. For example,

Contributing test - have accepted communication to the internet.

Contributing test - and have accepted communication from the internet.

Restrictive test - and include only if the inbound and outbound flow count has a percentage difference greater than 40. |
| include only if the time is between start time and end time inclusive | Filters communications within your network that occurred within a specific time range. This allows you to detect out-of-policy communications. For example, if your corporate policy allows FTP communications between 1 and 3 am, this tests can detect any attempts to use FTP to communicate outside of that time range. |

Test Name	Description
include only if the day of week is between start day and end day inclusive	Filters assets from the contributing test question based on network communications that occurred within a specific time range. This allows you to detect out-of-policy communications.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, **are susceptible to one of the following vulnerabilities**. This contributing rule containing a vulnerabilities parameter is required.
include only the following networks	Filters assets from a contributing test question that includes or excludes the configured networks.
include only the following asset building blocks	Filters assets from a contributing test question that are or are not associated with the configured asset building blocks.
include only the following asset saved searches	Filters assets from a contributing test question that are or are not associated with the asset saved search.
include only the following reference sets	Filters assets that are from a contributing test question that includes or excludes the configured reference sets.
include only the following IP addresses	Filters assets that are or are not associated with the configured IP addresses.
include only if the Microsoft Windows service pack for operating systems is below 0	Filters assets to determine if a Microsoft Windows service pack level for an operating system is below the level your company policy specifies.
include only if the Microsoft Windows security setting is less than 0	Filters assets to determine if a Microsoft Windows security setting is below the level your company policy specifies.
include only if the Microsoft Windows service equals status	Filters assets to determine if a Microsoft Windows service is unknown, boot, kernel, auto, demand, or disabled.
include only if the Microsoft Windows setting equals regular expressions	Filters assets to determine if a Microsoft Windows Setting is the specified regular expression.

Contributing questions for possible communication tests

The possible communication tests for assets include contributing questions and parameters that you can choose when you create a policy monitor test.

The following table lists and describes the contributing question parameters for possible communication tests.

Table 17. Possible communication question parameters for contributing tests

Test Name	Description
have accepted communication to any destination	Detects assets that have possible communications to or from any specified source or destination. For example, to determine if a critical server can possibly receive communications from any source, configure the test as follows:
	have accepted communication from any source.
	You can then apply a restrictive test to return if that critical server has received any communications on port 21. This allows you to detect out-of-policy communications for that critical server.
have accepted communication to destination networks	Detects assets that have possible communications to or from the configured network.
	This test allows you to define a start or end point to your question.
	For example, to identify the assets that have the possibility of communicating to the DMZ, configure the test as follows:
	have accepted communication from source <networks>
	You can use this test to detect out-of-policy communications.
have accepted communication to destination IP addresses	Detects assets that have possible communications to or from the configured IP address. This test allows you to specify a single IP address as a focus for possible communications. For example, if you want to identify all assets that can communicate to a specific compliance server, configure the test as follows:
	have accepted communications to destination <compliance server IP address>
have accepted communication to destination asset building blocks	Detects assets that have possible communications to or from the configured asset using building blocks. This test allows you to re-use building blocks defined in the QRadar Rules Wizard in your query. For example, if you want to identify all assets that can communicate to a Protected Assets, configure the test as follows:
	have accepted communications to destination `<BB:HostDefinition:Protected Assets>`
	For more information about rules and building blocks, see the *IBM Security QRadar SIEM Administration Guide*.

Table 17. Possible communication question parameters for contributing tests (continued)

Test Name	Description
have accepted communication to destination asset saved searches	Detects assets that have accepted communications to or from the assets that are returned by the saved search that you specify. A saved asset search must exist before you use this test. For information about creating and saving an asset search, see the *IBM Security QRadar SIEM Users Guide*
have accepted communication to destination reference sets	Detects if source or destination communication are possible to or from reference sets.
have accepted communication to the Internet	Detects if source or destination communications are possible to or from the Internet. Specify the **to** or **from** parameter, to consider communication traffic to the Internet or from the Internet.
are susceptible to one of the following vulnerabilities	Detects possible specific vulnerabilities. If you want to detect vulnerabilities of a particular type, use the test, **are susceptible to vulnerabilities with one of the following classifications**. Specify the vulnerabilities to which you want this test to apply. You can search for vulnerabilities using the OSVDB ID, CVE ID, Bugtraq ID, or title
are susceptible to vulnerabilities with one of the following classifications	A vulnerability can be associated with one or more vulnerability classification. This test filters all assets that have possible vulnerabilities with a Common Vulnerability Scoring System (CVSS) score, as specified. Configure the classifications parameter to identify the vulnerability classifications that you want this test to apply.
are susceptible to vulnerabilities with CVSS score greater than 5	A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of possible vulnerabilities. CVSS is composed of three metric groups: Base, Temporal, and Environmental. These metrics allow CVSS to define and communicate the fundamental characteristics of a vulnerability. This test filters assets in your network that include the configured CVSS value.
are susceptible to vulnerabilities disclosed after specified date	Filters assets in your network with a possible vulnerability that is disclosed after, before, or on the configured date.

Table 17. Possible communication question parameters for contributing tests (continued)

Test Name	Description
are susceptible to vulnerabilities on one of the following ports	Filters assets in your network with a possible vulnerability that is associated with the configured ports. Configure the ports parameter to identify assets that have possible vulnerabilities based on the specified port number.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more text entry. Configure the **text entries** parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Detects assets in your network with a vulnerability that matches the asset name, vendor, version or service based one or more regular expression. Configure the **regular expressions** parameter to identify the asset name, vendor, version or service you want this test to consider.
are susceptible to vulnerabilities contained in vulnerability saved searches	Detects risks that are associated with saved searches that are created in IBM Security QRadar Vulnerability Manager.

Deprecated contributing test questions

If a test is replaced with another test, it is hidden in policy monitor.

The following tests are hidden in the Policy Monitor:
- assets that are susceptible to vulnerabilities from the following vendors
- assets that are susceptible to vulnerabilities from the following services

These contributing tests have been replaced by other tests.

Restrictive question parameters for possible communication tests

Possible communication tests for assets include restrictive question parameters.

The following table lists and describes the restrictive question parameters for possible communication tests.

Table 18. Restrictive tests for possible communication tests

Test Name	Description
include only the following protocols	Filters assets that have or have not possibly communicated with the configured protocols, in conjunction with the other tests added to this question.

Table 18. Restrictive tests for possible communication tests (continued)

Test Name	Description
include only the following inbound ports	Filters assets that have or have not possibly communicated with the configured ports, in conjunction with the other tests added to this question.
include only ports other than the following inbound ports	Filters assets from a contributing test question that have or have not possibly communicated with ports other than the configured ports, in conjunction with the other tests added to this question.
include only if susceptible to vulnerabilities that are exploitable.	Filters assets from a contributing test question searching for possible specific vulnerabilities and restricts results to exploitable assets. This restrictive test does not contain configurable parameters, but is used in conjunction with the contributing test, **are susceptible to one of the following vulnerabilities**. This contributing rule containing a vulnerabilities parameter is required.
include only the following networks	Filters assets from a contributing test question that include only or exclude the configured networks.
include only the following asset building blocks	Filters assets from a contributing test question that include only or exclude the configured asset building blocks.
include only the following asset saved searches	Filters assets from a contributing test question that include only or exclude the associated asset saved search.
include only the following reference sets	Filters assets from a contributing test question that include only or exclude the configured
include only the following IP addresses	Filters assets Filters assets from a contributing test question that include only or exclude the configured IP addresses.
include only if the Microsoft Windows service pack for operating systems is below 0	Filters assets to determine if a Microsoft Windows service pack level for an operating system is below the level your company policy specifies.
include only if the Microsoft Windows security setting is less than 0	Filters assets to determine if a Microsoft Windows security setting is below the level your company policy specifies.
include only if the Microsoft Windows service equals status	Filters assets to determine if a Microsoft Windows service is unknown, boot, kernel, auto, demand, or disabled.
include only if the Microsoft Windows setting equals regular expressions	Filters assets to determine if a Microsoft Windows Setting is the specified regular expression.

Device/rules test questions

Devices/rules test questions are used to identify rules in a device that violate a defined policy that can introduced risk into the environment.

The device/rules test questions are described in the following table.

Table 19. Device/rules tests

Test Name	Description
allow connections to the following networks	Filters device rules and connections to or from the configured networks. For example, if you configure the test to allow communications to a network, the test filters all rules and connections that allow connections to the configured network.
allow connections to the following IP addresses	Filters device rules and connections to or from the configured IP addresses. For example, if you configure the test to allow communications to an IP address, the test filters all rules and connections that allow connections to the configured IP address.
allow connections to the following asset building blocks	Filters device rules and connections to or from the configured asset building block.
allow connections to the following reference sets	Filters device rules and connections to or from the configured reference sets.
allow connections using the following destination ports and protocols	Filters device rules and connections to or from the configured ports and protocols
allow connections using the following protocols	Filters device rules and connections to or from the configured protocols.
allow connections to the Internet	Filters device rules and connections to and from the Internet.
are one of the following devices	Filters all network devices to the configured devices. This test can filter based on devices that are or are not in the configured list.
are one of the following reference sets	Filters device rules based on the reference sets that you specify.
are one of the following networks	Filters device rules based on the networks that you specify.
are using one of the following adapters	Filters device rules based on the adapters that you specify.

Chapter 7. Investigate connections

A connection is a recording of a communication, including denied communications, between two unique IP addresses over a specific destination port, as detected over a specific time interval.

If two IP addresses communicate many times over the same interval on a port, only one communication is recorded, but the bytes communicated and the number of flows are totaled with the connection. At the end of the interval, the connection information is accumulated over the interval and is stored in the database.

Connections allows you to monitor and investigate network device connections or perform advanced searches. You can:

- Search connections
- Search a subset of connections
- Mark search results as a false positive to tune out false positive events from created offenses.
- View connection information grouped by various options
- Export connections in XML or CSV format
- Use the interactive graph to view connections in your network

Viewing connections

View connection information that is grouped by various options.

About this task

By default, the Connections window displays the following graphs:

- **Records Matched Over Time** graph provides time-series information that shows the number of connections based on time.
- **Connection Graph** that provides a visual representation of the connections retrieved.

Note: If a saved search is the default, the results for that saved search are displayed.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Select a time frame by selecting the **Start Time** and **End Time** parameters, or use the **View** list.

   In the table, right-click any cell (except cells from the **Last Packet Time** column) for a menu, to apply more filtering or to **View Connection Events**.

Example

The Connections window displays the following information:

Table 20. Connections window - default

Parameter	Description
Current Filters	This parameter displays only after you apply a filter. Details of the filter that is applied to the search result are displayed on top. To clear these filter values, click **Clear Filter**.
View	From the list, select the time range that you want to filter. Use the **Expand** option to adjust the time range.
Current Statistics	Current statistics include the following parameters: **Total Results** - The total number of results that matched your search criteria. **Data Files Searched** - The total number of data files searched during the specified time span. **Compressed Data Files Searched** - The total number of compressed data files searched within the specified time span. **Index File Count** - The total number of index files searched during the specified time span. **Duration** - The duration of search. **Current Statistics** are helpful for troubleshooting. When you contact Customer Support to troubleshoot an issue, you might be asked to provide current statistical information. Click the arrow next to **Current Statistics** to display or hide the statistics.
Charts	Displays charts that represent the records that are matched by the time interval and/or grouping option. Click **(Hide Charts)** if you want to remove the graph from your display. **Note:** Remove Firefox *Adblock Plus* if it prevents charts from displaying in Firefox.
Last Packet Time	The date and time of the last processed packet for this connection.
Source Type	The **Source Type** for this connection, which can be: `Host` or `Remote`.

Table 20. Connections window - default (continued)

Parameter	Description
Source	The following are options for the **Source**: **IP address** - The IP address for the source of this connection. If the **Source Type** is **Host**, the IP address is displayed. **Country** - The source country (with the country flag) for this connection. The country flag is only displayed if the Source Type is remote.
Destination Type	The options for **Destination Type** are: `Host` or `Remote`.
Destination	The options for **Destination** are: `IP address` - If the Destination Type is host, the IP address is displayed. `Country` - The destination country (with the country flag) for this connection. The country flag is only displayed if the **Destination Type** is remote.
Protocol	The protocol that is used for this connection.
Destination Port	The destination port for this connection.
Flow Application	The flow application that generated the connection.
Flow Source	The source of flows that are associated with this connection. This parameter applies only to accepted connections.
Flow Count	The total number of flows that are associated with this connection.
Flow Source Bytes	The total number of flow source bytes associated with this connection.
Flow Destination Bytes	The total number of destination bytes associated with this connection.
Log Source	The source of events that contribute to this connection.
Event Count	The total number of events that are detected for the connection.
Connection Type	The options for connection type are: **Allow** or **Deny**.

Use graphs to view connection data

You can view connection data using various chart options. By default, you can view data using records matched over time and connection graph.

Records matched over time is an option that indicates the number of connections based on time.

A connection graph provides a visual representation of the connection retrieved. If you want to further investigate connections using the connection graph, see Using the connection graph.

Graph options available for grouped connections are table, bar and pie. For more information about searching connections, see Search for connections.

If you use an Adblock Plus browser extension with a Mozilla Firefox web browser, the charts might not display properly. For the charts to display, you must remove the Adblock Plus browser extension. For more information about removing add-ons, see your web browser documentation.

Using the time series graph

Time series charts are graphical representations of your connections over time; peaks and valleys that display, depict high and low connection activity.

Before you begin

If you previously saved a search to be the default, the results for that saved search display on the Connections page. If that search included Group By options selected in the Advanced View Definitions box, the Time Series chart is not available. You must clear the search criteria before continuing.

About this task

Time series charts are useful for short-term and long-term trending of data. Using time series charts, you can access, navigate, and investigate connections from various views and perspectives.

The following table provides functions you can use to view time series charts.

Table 21. Time series chart functions

If you want to	Then
View connections in greater detail	Magnifying the data in a time series chart allows you to investigate smaller time segments of the connections. You can magnify the time series chart using one of the following options:
	Press the Shift key and click on the chart at the time you want to investigate.
	Press the Ctrl and Shift keys while you click and drag the mouse pointer over the range of time you want to view.
	Move your mouse pointer over the chart and press the Up arrow on your keyboard.
	Move your mouse pointer over the chart and then use your mouse wheel to zoom in (roll the mouse wheel up).
	After you magnify a time series chart, the chart refreshes to display a smaller time segment.

Table 21. Time series chart functions (continued)

If you want to	Then
View a larger time span of connections	Including additional time ranges in the time series chart allows you to investigate larger time segments or return to the maximum time range. You can view a time range using one of the following options: Click Max at the top left corner of the chart or press the Home key to return to the maximum time range. Move your mouse pointer over the chart and press the down arrow on your keyboard. Move your mouse pointer over the plot chart and then use your mouse wheel to zoom out (roll the mouse wheel down).
Scan the chart	To view the chart to determine information at each data point: Click and drag the chart to scan the time line. Press the Page Up key to move the time line a full page to the left. Press the left arrow key to move the time line one half page to the left. Press the Page Down key to move the time line a full page to the right. Press the right arrow key to move the time line one half page to the right

Procedure

Procedure
1. Click the Risks tab.
2. On the navigation menu, click **Connections**.
3. In the charts pane, click the **Configure** icon.
4. Using the **Chart Type** drop-down list, select Time Series.
5. Using the interactive time series charts, you can navigate through a time line to investigate connections.
6. To refresh the information in the graph, click Update Details.

Use connection graph to view network connections

The connection graph provides a visual representation of the connections in your network.

The graph that is displayed in the Connections window is not interactive. If you click the graph, the Radial Data Viewer window is displayed. The Radial Data Viewer window allows you to manipulate the graph, as required.

By default, the graph displays your network connections as follows:
- Only allowed connections are displayed.
- All local IP addresses are collapsed to show only leaf networks.
- All country nodes are collapsed to a node named Remote Countries.
- All remote network nodes are collapsed to one node named Remote Networks.
- Preview thumbnail view of the graph displays a portion of the main graph. This is useful for large graphs.

The Radial Data Viewer includes several menu options, including:

Table 22. Radial Data Viewer menu options

Menu Option	Description
Connection Type	By default, the radial graph displays accepted connections. If you want to view denied connections, select Deny from the **Connection Type** drop-down list.
Undo	Collapses the last node expansion. If you want to undo multiple expansions, click the Undo button for each expansion.
Download	Click **Download** to save the current topology as a JPEG image file or a Visio drawing file (VDX). To download and save the current topology as a Visio drawing file (VDX), the minimum software version you require is Microsoft Visio Standard 2010.

The following table provides additional functions to view connections including:

Table 23. Radial Data Viewer functions

If you want to	Then
Zoom in or zoom out	Use the slider on the top-right side of the graph to change the scale.
Distribute nodes on the graph to view additional details	Drag the node to the preferred location to distribute nodes on the graph.
Expand a network node	Double-click the node to expand and view assets for that node. The node expands to include the specific assets to which that node was communicating. By default, this expansion is limited to the first 100 assets of the network.
View additional details regarding a connection	Point your mouse over the connection line to view additional details. If the connection is between a network node to a remote network or remote country, right-click to display the following **Source** and **View Flows** menus: If the connection is between two IP addresses, the source, destination, and port information is displayed when you click the connection line.

Table 23. Radial Data Viewer functions (continued)

If you want to	Then
Determine the amount of data involved in the connection	The thickness of the line in the graph indicates the amount of data involved in the connection. A thicker line indicates a greater amount of data. This information is based on the amount of bytes involved in the communication
Highlight a connection path	Point your mouse over the connection line. If the connection is allowed, the path highlights green. If the connection is denied, the path highlights red.
Determine the connection path for a particular node	Pointer your mouse over the node. If the node is allowed, the path to the node and the node highlight in green. If the node is denied, the path to the node and the node highlights in red.
Change graph view	Using the preview thumbnail, move the thumbnail to the portion of the graph you want to display.

Using pie, bar, and table charts

You can view connections data using a pie, bar, or table chart.

About this task

The pie, bar, and table chart options only display if the search includes Group By options selected in the Advanced View Definition options.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.

   Note: The default saved search results display.
3. Perform a search.
4. In the charts pane, click the **Configuration** icon.
5. Configure the parameters:

Option	Description
Value to Graph	Using the **Value to Graph** list, select the object type to which you want to graph on the chart. Options include all normalized and custom flow parameters included in your search parameters.
Chart Type	Using the **Chart Type** list, select the chart type you want to view. Options include: **Table** - Displays data in a table. **Bar** - Displays data in a bar chart. **Pie** - Displays data in a pie chart.

6. Click **Save**.

The data does not refresh automatically, unless your search criteria is displayed to automatically display details.

7. To refresh the data, click **Update Details**.

Search for connections

You can search connections using specific criteria and display connections that match the search criteria in a results list. You can create a new search or load a previously saved set of search criteria.

Procedure

1. Click the **Risks** tab.

2. On the navigation menu, click **Connections**.

   If applicable, the default saved search results display.

3. Using the **Search** list, select **New Search**.

4. If you want to load a previously saved search, use one of the following options:

   a. From the **Group** list, select the group to which the saved search is associated.

   b. From the **Available Saved Searches** list, select the saved search you want to load.

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

   d. Click **Load**.

   e. In the **Edit Search** pane, select the options you want for this search.

Option	Description
Include in my Quick Searches	Include this search in your Quick Search items.
Include in my Dashboard	Include the data from your saved search in your dashboard. This parameter is only available if the search is grouped.
Set as Default	Set this search as your default search.
Share with Everyone	Share these search requirements with all other IBM Security QRadar Risk Manager users.

5. In the Time Range pane, select an option for the time range you want to capture for this search.

Option	Description
Recent	Using the list, specify the time range you want to filter.
Specific Interval	Using the calendar, specify the date and time range you want to filter.

6. If you are finished configuring the search and want to view the results, click Search.

7. In the Search Parameters pane, define your specific search criteria:

a. Using the first list, select an attribute on which you want to search. For example, Connection Type, Source Network, or Direction.

b. Using the second list, select the modifier you want to use for the search. The list of modifiers that display depends on the attribute selected in the first list.

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

d. Click **Add Filter**.

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

f. If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to the next step.

8. If you want to automatically save the search results when the search is completed, select the Save results when search is complete check box and specify a name.

9. If you are finished configuring the search and want to view the results, click **Search**. Otherwise, proceed to next step.

10. Using the Column Definition pane, define the columns and column layout you want to use to view the results:

a. Using the **Display** list, select the view you want to associate with this search.

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

11. Click **Search**.

Saving search criteria

You can create a search by specifying search criteria, and you can save the search for future use.

About this task

You can customize the columns that display in the search results. These options are available in the Column Definition section and are called Advanced View Definition options.

Table 24. Advanced View Definition options

Parameter	Description
Type Column or Select from List	Filters the columns in the Available Columns list. Type the name of the column you want to locate or type a keyword to display a list of column names that include that keyword. For example, type **Source** to display a list of columns that include Source in the column name.
Available Columns	Lists available columns associated with the selected view. Columns that are currently in use for this saved search are highlighted and displayed in the **Columns** list.

Table 24. Advanced View Definition options (continued)

Parameter	Description
Add and remove column buttons (top set)	The top set of buttons allows you to customize the **Group By** list. **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** button. **Remove Column** - Select one or more columns from the **Group By** list and click the **Remove Column** button.
Add and remove column buttons (bottom set)	The bottom set of buttons allows you to customize the **Columns** list. **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** button. **Remove Column** - Select one or more columns from the **Columns** list and click the **Remove Column** button.
Group By	Specifies the columns from which the saved search groups the results. You can further customize the **Group By** list using the following options: **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. The priority list specifies in which order the results are grouped. The search results will group by the first column in the **Group By** list and then group by the next column on the list.
Columns	Specifies columns chosen for the search. The columns are loaded from a saved search. You can customize the **Columns** list by selecting columns from the **Available Columns** list. You can further customize the **Columns** list by using the following options: **Move Up** - Select a column and move it up through the priority list using the move up button. **Move Down** - Select a column and move it down through the priority list using the move down button. If the column type is numeric or time and there is an entry in the **Group By** list, the column includes a drop-down list to allow you to choose how you want to group the column.

Table 24. Advanced View Definition options (continued)

Parameter	Description
Order By	Using the first list, specify the column by which you want to sort the search results. Then, using the second list, specify the order you want to display for the search results: **Descending** or **Ascending**.

Procedure

1. Click the **Risk**s tab.
2. On the navigation menu, click **Connections**.
3. Perform a search.
4. Click **Save Criteria**.
5. Configure values for the following parameters:

Option	Description
Search Name	Type a name you want to assign to this search criteria.
Assign Search to Group(s)	The group you want to assign to this saved search. If you do not select a group, this saved search is assigned to the Other group by default.
Timespan options	Choose one of the following options: Recent - Using the drop-down list, specify the time range you want to filter. Specific Interval - Using the calendar, specify the date and time range you want to filter.
Include in my Quick Searches	Select the check box if you want to include this search in your Quick Search items, which is available from the **Search** drop-down list.
Include in my Dashboard	Select the check box if you want to include the data from your saved search in your Dashboard. This parameter is only displayed if the search is grouped.
Set as Default	Select the check box if you want to set this search as your default search.
Share with Everyone	Select the check box if you want to share these search requirements with all other IBM Security QRadar Risk Manager users.

6. Click **OK**.

Performing a sub-search

Each time you perform a search, the entire database is queried for connections that match your criteria. This process might take an extended period of time, depending on the size of your database.

About this task

A sub-search allows you to search within a set of completed search results. You can refine your search results without searching the database again. A sub-search is not available for grouped searches or searches in progress.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Perform a search. The search results are displayed. Additional searches use the dataset from the previous search when sub-searches are performed.
4. To add a filter, perform the following steps:
   a. Click **Add Filter**.
   b. Using the first list, select an attribute on which you want to search.
   c. Using the second list, select the modifier you want to use for the search. The list of modifiers that display depends on the attribute selected in the first list.
   d. In the text field, type specific information related to your search.
   e. Click **Add Filter**.

      Note: If the search remains in progress, partial results are displayed. The Original Filter pane indicates the filter from which the original search was based. The Current Filter pane indicates the filter applied to the sub-search.

      Tip: You can clear sub-search filters without restarting the original search. Click the Clear Filter link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the original search is relaunched.
5. Click **Save Criteria** to save the sub-search.

Results

If you delete the original search, you can access the saved sub-search. If you add a filter, the sub-search searches the entire database since the search function no longer bases the search on a previously searched dataset.

Manage search results

You can perform multiple connection searches while navigating to other interfaces.

About this task

You can configure the search feature to send you an email notification when a search is complete. At any time while a search is in progress, you can view partial results of a search in progress.

The search results toolbar provides the following options:

Parameter	Description
New Search	Click **New Search** to create a new search. When you click this button, the search window is displayed.

Parameter	Description
Save Results	Click **Save Results** to save search results. This option is only enabled when you have selected a row in the Manage Search Results list.
Cancel	Click **Cancel** to cancel searches that are in progress or are queued to start.
Delete	Click **Delete** to delete a search result.
Notify	Select the search(es) for which you want to receive notification, and then click **Notify** to enable email notification when the search is complete.
View	From the drop-down list, specify which search results you want to list in the search results window. The options are: Saved Search Results All Search Results Canceled/Erroneous Searches Searches in Progress

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. From the menu, select **Search** > **Manage Search Results**.

Saving Search Results
You can save your search results.

Procedure
1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. Perform a connection search or sub-search.
4. From the Search Results window, select **Search** > **Manage Search Results** and select a search result.
5. Click **Save Results**.
6. Type a name for the search results.
7. Click **OK**.

Canceling a search
You can cancel one or more searches.

About this task

If a search is in progress when canceled, the accumulated results, up until the cancellation of the search, are maintained.

Procedure

1. From the Manage Search Results window, select the queued or in progress search result you want to cancel. You can select multiple searches to cancel.
2. Click **Cancel Search**.
3. Click **Yes**.

Deleting a search

You can delete a search.

Procedure

1. From the Manage Search Results window, select the search result you want to delete.
2. Click **Delete**.
3. Click **Yes**.

Exporting connections

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

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Connections**.
3. If you want to export the connection in XML format, select **Actions** > **Export to XML**.
4. If you want to export the connection in CSV format, select **Actions > Export to CSV**.
5. If you want to resume your activities, click **Notify When Done**.

Chapter 8. Log source mapping

To monitor the trigger frequency of firewall rules and enable topology event searches, IBM Security QRadar Risk Manager identifies QRadar log sources.

By understanding firewall rules you can maintain firewall efficiency and prevent security risks.

A maximum of 255 devices can be mapped to a log source in QRadar Risk Manager, but devices can have multiple log sources.

Log source mapping display options

If you configured your network device as a QRadar log source, the Configuration Monitor page displays one of the following entries in the **Log Source** column:

- **Auto-Mapped** - If QRadar Risk Manager identifies and maps the log source to the device automatically.
- **Username** - If an administrator manually added or edited a log source.
- **Blank** - If QRadar Risk Manager is unable to identify a log source for the device, the **Log Source** column shows no value. You can manually create a log source mapping.

For more information about configuring log sources, see the *IBM Security QRadar Log Sources User Guide*.

Creating or editing a log source mapping

If IBM Security QRadar Risk Manager cannot identify a log source in QRadar, you can configure a log source mapping.

Procedure

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. Click the device without a log source mapping.
4. On the toolbar, click **Action** > **Log Source Mapping** > **Create/Edit Log Source Mapping**.
5. In the **Log Source Groups** list, select a group.
6. In the **Log Sources** list, select a log source and click (**>**).
7. Click **OK**.

Chapter 9. Investigating your network device configurations

In IBM Security QRadar Risk Manager, you can manage the efficiency of your network devices, investigate firewall rules, and identify security risks that are created by invalid firewall rules.

Procedure

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. To search your network devices, enter an IP address or Host Name in the **Input IP Address or Host Name** field.
4. Double-click the device that you want to investigate.

   The rule **Event Count** column displays the firewall rule trigger frequency. A zero event count rule is displayed for one of the following reasons:

   - A rule is not triggered and might cause a security risk. You can investigate your firewall device and remove any rules that are not triggered.
   - A QRadar log source mapping is not configured.
5. To search the rules, on the **Rules** toolbar, click **Search** > **New Search**.

   If an icon is displayed in the **Status** column, you can hover your mouse over the status icon to display more information.
6. To investigate the device interfaces, on the toolbar, click **Interfaces**.
7. To investigate access control list (ACL) device rules, on the toolbar, click **ACLs**.

   Each access control list defines the interfaces over which the devices on your network are communicating. When the conditions of an ACL are met, the rules that are associated with an ACL are triggered. Each rule is tested to allow or deny communication between devices.
8. To investigate network address translation (NAT) device rules, on the toolbar, click **NAT**.

   The **Phase** column specifies when to trigger the NAT rule, for example, before or after routing.
9. To investigate the history or compare device configurations, on the toolbar, click **History**.

   You can view device rules in a normalized comparison view or the raw device configuration. The normalized device configuration is a graphical comparison that shows added, deleted, or modified rules between devices. The raw device configuration is an XML or plain text view of the device file.

Searching device rules

In IBM Security QRadar Risk Manager, you can search for rules that changed on the devices in your topology. You can also discover rule changes that occur between device configuration backups.

The results that are returned for a rule search are based on the configuration source management backup of your device. To ensure that rule searches provide up-to-date information, you can schedule device backups in your firewall policy update page.

Procedure

1. Click the **Risks** tab.
2. In the navigation pane, click **Configuration Monitor**.
3. Double-click a device from the Configuration Monitor page.
4. On the Rules pane toolbar, click **Search** > **New Search**.
5. In the **Search Criteria** area, click a time range.
6. To search your device rules, choose from the following options:
   - To search for **Shadowed**, **Deleted** or **Other** rules, click a status option.

     By default all status options are enabled. To search for shadow rules only, clear the **Deleted** and **Other** options.
   - To search for an access control list (ACL), type in the **List** field.
   - To search on the order number of the rule entry, type a numeric value in the **Entry** field.
   - To search for a source or destination, type an IP address, CIDR address, host name, or object group reference.
   - To search for ports or object group references, type in the **Service** field.

     The service can include port ranges, such as 100-200, or port expressions, such as 80(TCP). If the port is negated, the port information also includes an exclamation mark and might be surrounded by parenthesis, for example, !(100-200) or !80(TCP).
   - To search for vulnerability rule information as defined by the IPS device, type in the **Signature** field.
   - To search for applications by adapter, click **Select Applications**, then type an adapter or application name.
7. Click **Search**.

Comparing the configuration of your network devices

In IBM Security QRadar Risk Manager, device configurations can be compared to each other by comparing multiple backups on a single device or by comparing one network device backup to another.

Common configuration types can include the following items:
- **Standard Element Document** - Standard Element Document (SED) files are XML data files that contain information about your network device. Individual SED (standard element document) files are viewed in their raw XML format. If a SED (standard element document) file is compared to another SED (standard element document) file, then the view is normalized to display the rule differences.
- **Config** - Configuration files are provided by certain network devices, depending on the device manufacturer. You can view a configuration file by double-clicking it.

Depending on the information that the adapter collects for your device, several other configuration types might be displayed. These files are displayed in plain text view when double-clicked.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. Double-click any device to view the detailed configuration information.
4. Click **History** to view the history for this device.

5. To compare two configurations on a single device:
   a. Select a primary configuration.
   b. Press the Ctrl key and select a second configuration for comparison.
   c. In the History pane, click **Compare Selected**.

      If the comparison files are standard element documents (SEDs), then the Normalized Device Configuration Comparison window shows rule differences between the backups.

      When you compare normalized configurations, the color of the text shows the following device updates:
      • A green dotted outline shows a rule or configuration that was added to the device.
      • A red dashed outline shows a rule or configuration that was deleted from the device.
      • A yellow solid outline shows a rule or configuration that was modified on the device.
   d. To view the raw configuration differences, click **View Raw Comparison**.

      If the comparison is a configuration file or another backup type, then the raw comparison is displayed.
6. To compare two configurations on different devices:
   a. Select a primary configuration from a device.
   b. Click **Mark for Comparison**.
   c. From the navigation menu, select **All Devices** to return to the device list.
   d. Double-click the device to compare and click **History**.
   e. Select a configuration that you want to compare with the marked configuration.
   f. Click **Compare with Marked**.
   g. To view the raw configuration differences, click **View Raw Comparison**.

Chapter 10. Filtering device rules by user or group

In QRadar Risk Manager, you can view and filter your device rules by user or group.

About this task

Search by user or group rule interaction, and get a sense of how the typical user or group interacts in your network. Knowing your users' rule interactions in your network is helpful in discovering any errant behavior, and helps you in formulating efficient rule policies in your network.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, click **Configuration Monitor**.
3. From the **Device List** table, double-click the table row for your device.

   From the **User(s)/Group(s)** column in the rules table, you can view your users and groups.
4. From the Rules pane, click **Search** > **New Search**.
5. Type the user or group name in the **User or Group** field.
6. Click **Search**.

   If the search string matches any part of a user or group name, rules that are linked to the user or group name are displayed.

   Use the rule information to establish benchmarks or profiles for user rule interaction, which can be used to optimize rule policies in your network.

Chapter 11. Managing IBM Security QRadar Risk Manager reports

You can create, edit, distribute, and manage reports for your network devices. Detailed reports on firewall rules and connections between devices are often required to satisfy various regulatory standards, such as PCI compliance.

The following report options are specific to QRadar Risk Manager:

Table 25. Report options for QRadar Risk Manager

Report option	Description
Connections	The connection diagrams for your network devices that occurred during your specified time frame.
Device rules	The rules configured on your network device during your specified time frame. You can view the following rule types for one or many network devices using this report option: Most used accept rules Most used deny rules Least used accept Least used deny rules Shadowed rules Unused object rules
Device unused objects	Produces a table with the name, configuration date/time, and a definition for any object reference groups that are not in use on the device. An object reference group is a generic term used to describe a collection of IP addresses, CIDR addresses, host names, ports, or other device parameters which are grouped together and assigned to rules on the device.

Manually generating a report

Reports can be started manually. If you start multiple reports manually, the reports are added to a queue and labeled with their queue position.

About this task

Manually generating a report does not reset the existing report schedule. For example, if you generate a weekly report for most active firewall denies, then manually generate the report, the weekly report still generates on the schedule you initially configured.

When a report generates, the **Next Run Time** column displays one of the three following messages:

- **Generating** - The report is generating.
- **Queued (position in the queue)**- The report is queued for generation. The message indicates the position the report is in the queue. For example, 1 of 3.
- **(x hour(s) x min(s)y sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to generate.
3. Click **Run Report**.
4. Optional. Click **Refresh** to refresh the view, including the information in the **Next Run Time** column.

What to do next

After the report generates, you can view the generated report from the **Generated Reports** column.

Use the report wizard

You can use the Report Wizard to create a new report. The Report Wizard provides a step-by-step guide on how to design, schedule, and generate reports.

The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder and location for content in your report
- **Content** - Defines the report data IBM Security QRadar Risk Manager includes in chart for the container

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

The scheduled time must elapse for reports that generate weekly or monthly before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires 7 days to build the data. This search returns results after 7 days elapse.

Creating a report

You can create reports for a specific interval and can choose a chart type.

About this task

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

You can specify Report Console or email for report distribution options. The following table describes the parameters on for these distribution options.

Table 26. Generated report distribution options

Option	Description
Report Console	Select this check box to send the generated report to the **Reports** tab. This is the default distribution channel.
Select the users that should be able to view the generated report.	This option is only displayed after you select the **Report Console** check box. From the list of users, select the IBM Security QRadar Risk Manager users you want to grant permission to view the generated reports. You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the *IBM Security QRadar SIEM Administration Guide*.
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all QRadar Risk Manager users to view the generated reports. You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the *IBM Security QRadar SIEM Administration Guide*.
Email	Select this check box if you want to distribute the generated report using email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter is 255. Email recipients receive this email from no_reply_reports@qradar.
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **Email** check box. Select this check box to send the generated report as an attachment.

Table 26. Generated report distribution options (continued)

Option	Description
Include link to Report Console	This option is only displayed after you select the **Email** check box. Select this check box to include a link the Report Console in the email.

Procedure

1. Click the **Reports** tab.
2. From the **Actions** list, select **Create**.
3. Click **Next** to move to the next page of the Report Wizard.
4. Select the frequency for the reporting schedule.
5. In the Allow this report to generate manually pane, select **Yes** to enable or **No** to disable manual generation of this report. This option is not available for manually generated reports.
6. Click **Next**.
7. Choose a layout of your report, and then click **Next**.
8. Enter a report title. The title can be up to 100 characters in length. Do not use special characters.
9. Choose a logo. The QRadar logo is the default logo. For more information about branding your report, see the *IBM Security QRadar SIEM Administration Guide*.
10. From the **Chart Type** list, select one of the QRadar Risk Manager specific reports.
11. Configure the report data for your chart.
12. Click **Save Container Details**.
13. Click **Next**.
14. Select report formats. You can select multiple options.

    Note: Device Rules and Unused Object Rules reports only support the PDF, HTML, and RTF report formats.
15. Click **Next**.
16. Select the distribution channels that you want for your report.
17. Click **Next**.
18. Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.
19. Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *IBM Security QRadar SIEM Administration Guide*.
20. Optional. Select yes to run this report when the wizard setup is complete. Click **Next** to view the report summary. You can select the tabs available on the summary report to preview the report selections.
21. Click **Finish**.

Results

The report immediately generates. If you cleared the **Would you like to run the report now** check box on the final page of the wizard, the report is saved and generates as scheduled.

The report title is the default title for the generated report. If you reconfigure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Editing a report

You can edit a report to adjust a report schedule, layout, configuration, title, format, and delivery method. You can either edit existing reports or edit a default report.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to edit.
3. From the **Actions** list, select **Edit**.
4. Select the frequency for the new reporting schedule.
5. In the Allow this report to generate manually pane, select one of the following options:
   - **Yes** - Enables manual generation of this report.
   - **No** - Disables manual generation of this report.
6. Click **Next** to move to the next page of the Report Wizard.
7. Configure the layout of your report:
   a. From the **Orientation** list, select the page orientation.
   b. Select a layout option for your IBM Security QRadar Risk Manager report.
   c. Click **Next**.
8. Specify values for the following parameters:
   - **Report Title** - Type a report title. The title can be up to 100 characters in length. Do not use special characters.
   - **Logo** - From the list, select a logo. The QRadar logo is the default logo. For more information about branding your report, see the *IBM Security QRadar SIEM Administration Guide*.
9. Configure the container for your report data:
   a. Click **Define**.
   b. Configure the report data for your chart.
   c. Click **Save Container Details**.
   d. If required, repeat steps these steps to edit additional containers.
   e. Click **Next** to move to the next page of the Report Wizard.
10. Click **Next** to move to the next step of the Report Wizard.
11. Select the check boxes for the report formats. You can select more than one option.

    Note: QRadar Risk Manager-specific reports, such as Device Rule and Device Unused Object reports only support PDF, HTML, and RTF formats.
12. Click **Next** to move to the next page of the Report Wizard.
13. Select the distribution channels for your report.

14. Click **Next** to go to the final step of the Report Wizard.
15. Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.
16. Select the groups to which you want to assign this report. For more information about groups, see Managing Reports in the *IBM Security QRadar SIEM Administration Guide*.
17. Optional. Select yes to run this report when the wizard setup is complete.
18. Click **Next** to view the report summary. The Report Summary page is displayed, providing the details for the report. You can select the tabs available on the summary report to preview the report selections.
19. Click **Finish**.

Duplicating a report

You can duplicate any report.

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

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule.

Before you begin

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user

About this task

Any updates that the user makes to a shared report does not affect the original version of the report.

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

   If no users with appropriate access are available, a message is displayed.
5. Click **Share**.

   For more information about reports, see the *IBM Security QRadar SIEM Users Guide*.

Configuring charts

The chart type determines the data configured and displayed in the chart. You can create several charts for specific to data collected by devices in IBM Security QRadar Risk Manager.

The following chart types are specific to QRadar Risk Manager:
- Connection
- Device rules
- Device Unused Objects

Connection charts

You can use the Connections chart to view network connection information. You can base your charts on data from saved connection searches from the Risks tab.

You can customize the data that you want to display in the generated report. You can configure the chart to plot data over a configurable time period. This functionality helps you to detect connection trends.

The following table provides configuration information for the Connections Chart container.

Table 27. Connections chart parameters

Parameter	Description
Container Details - Connections	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created subtitle. Type a title to a maximum of 100 characters.
Graph Type	From the list, select the type of graph to display on the generated report. Options include:
	Bar - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search.
	Line - Displays the data in a line chart.
	Pie - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search.
	Stacked Bar - Displays the data in a stacked bar chart.
	Stacked Line - Displays the data in a stacked line chart.
	Table - Displays the data in table format. The **Table** option is only available for the full page width container only.

Table 27. Connections chart parameters (continued)

Parameter	Description
Graph	From the list, select the number of connections to be displayed in the generated report.
Manual Scheduling	The Manual Scheduling pane is displayed only if you selected the **Manually** scheduling option in the Report Wizard. To create a manual schedule: 1. From the **From** list box, type the start date that you want for the report, or select the date by using the **Calender** icon. The default is the current date. 2. From the list boxes, select the start time that you want for the report. Time is available in half-hour increments. The default is 1:00 am. 3. From the **To** list, type the end date that you want for the report, or select the date by using the **Calender** icon. The default is the current date. 4. From the lists, select the end time that you want for the report. Time is available in half-hour increments. The default is 1:00 am.
Hourly Scheduling	The Hourly Scheduling pane is displayed only if you selected the **Hourly** scheduling option in the Report Wizard. Hourly Scheduling automatically graphs all data from the previous hour.
Daily Scheduling	The Daily Scheduling pane is displayed only if you selected the **Daily** scheduling option in the Report Wizard. Choose one of the following options: **All data from previous day (24 hours)** **Data of previous day from** - From the lists, select the time period that you want for the generated report. Time is available in half-hour increments. The default is 1:00 am.
Weekly Scheduling	The Weekly Scheduling pane is displayed only if you selected the **Weekly** scheduling option in the Report Wizard. Choose one of the following options: **All data from previous week** **All Data from previous week from** - From the lists, select the time period that you want for the generated report. The default is Sunday.

Table 27. Connections chart parameters (continued)

Parameter	Description
Monthly Scheduling	The Monthly Scheduling pane is displayed only if you selected the **Monthly** scheduling option in the Report Wizard. Choose one of the following options: **All data from previous month** **Data from previous month from the** - From the lists, select the time period that you want for the generated report. The default is 1st to 31st.
Graph Content	
Group	From the list, select a saved search group to display the saved searches that belong to that group in the **Available Saved Searches** list.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type DMZ to display a list of all searches that include DMZ in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed. However, you can filter the list by selecting a group from the **Group** list or typing the name of a known saved search in the **Type Saved Search or Select from List** field.
Create New Connection Search	Click **Create New Connection Search** to create a new search.

Device Rules charts

You can use the Device Rules chart to view firewall rules and the event count of firewall rules triggered in your network.

Device Rule reports allows you to create a report for the following firewall rules:
- Most active accept device rules
- Most active deny device rules
- Least active accept device rules
- Least active deny device rules
- Unused device rules
- Shadowed device rules

The reports that you generate allow you to understand what rules are accepted, denied, unused, or untriggered across a single device, a specific adapter, or

multiple devices. Reports allow IBM Security QRadar Risk Manager to automate reporting about the status of your device rules and display the reports on the IBM Security QRadar SIEM Console.

This functionality helps you identify how rules are used on your network devices.

To create a Device Rules Chart container, configure values for the following parameters:

Table 28. Device Rules Chart parameters

Parameter	Description
Container Details - Device Rules	
Limit Rules to Top	From the list, select the number of rules to be displayed in the generated report. For example, if you limit your report to the top 10 rules, then create a report for most used accept rules across all devices, the report returns 10 results. The results contain a list of the 10 most used accept rules based on the event count across all devices that are visible to QRadar Risk Manager.

Table 28. Device Rules Chart parameters (continued)

Parameter	Description
Type	Select the type of device rules to display in the report. Options include: **Most Used Accept Rules** - Displays the most used accept rules by event count for a single device or a group of devices. This report lists the rules with highest accepted event counts, in descending order, for the time frame you specified in the report. **Most Used Deny Rules** - Displays the most used deny rules by event count for a single device or a group of devices. This report lists the rules with the highest deny event counts, in descending order, for the time frame you specified in the report. **Unused Rules** - Displays any rules for a single device or a group of devices that are unused. Unused rules have zero event counts for the time frame you specified for the report. **Least Used Accept Rules** - Displays the least used accept rules for a single device or a group of devices. This report lists rules with the lowest accept event counts, in ascending order, for the time frame you specified in the report. **Least Used Deny Rules** - Displays the least used deny rules for a single device or a group of devices. This report lists rules with the lowest denied event counts, in ascending order, for the time frame you specified in the report. **Shadowed Rules** - Displays any rules for a single device that can never trigger because the rule is blocked by a proceeding rule. The results display a table of the rule creating the shadow and any the rules that can never trigger on your device because they are shadowed by a proceeding rule on the device. **Note:** Shadowed rule reports can only be run against a single device. These rules have zero event counts for the time frame you specified for the report and are identified with an icon in the Status column.

Table 28. Device Rules Chart parameters (continued)

Parameter	Description
Date/Time Range	Select the time frame for your report. The options include:
	Current Configuration - The results of the Device Rules report is based on the rules that exist in the current device configuration. This report displays rules and event counts for the existing device configuration.
	The current configuration for a device is based on the last time Configuration Source Management backed up your network device.
	Interval - The results of the Device Rules report is based on the rules that existed during the time frame of the interval. This report displays rules and event counts for the specified interval from the last hour to 30 days.
	Specific Range - The results of the Device Rules report is based on the rules that existed between the start time and end time of the time range. This report displays rules and event counts for the specified time frame.
Timezone	Select the timezone you want to use as a basis for your report. The default timezone is based on the configuration of your QRadar SIEM Console.
	When configuring the Timezone parameter for your report, consider the location of the devices associated with the reported data. If the report uses data spanning multiple time zones, the data used for the report is based on the specific time range of the time zone.
	For example, if your QRadar SIEM Console is configured for Eastern Standard Time (EST) and you schedule a daily report between 1pm and 3pm and set the timezone as Central Standard Time (CST), the results in the report contains information from 2pm and 4pm EST.

Table 28. Device Rules Chart parameters (continued)

Parameter	Description
Targeted Data Selection	Targeted Data Selection is used to filter the Date/Time Range to a specific value. Using the Targeted Data Selection options, you can create a report to view your device rules over a custom defined period of time, with the option to only include data from the hours and days that you select. For example, you can schedule a report to run from October 1 to October 31 and view your most active, least active or unused rules and their rule counts that occur during your business hours, such as Monday to Friday, 8 AM to 9 PM. **Note:** The filter details only display when you select the **Targeted Data Selection** check box in the Report Wizard.
Format	Select the format for your device rules report. The options include: **One aggregate report for specified devices** - This report format aggregates the report data across multiple devices. For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules across all of the devices you have selected for the report. This report returns 10 results in total for the report. **One report per device** - This report format displays the report data for one device. For example, if you create a report to display the top ten most denied rules, then an aggregate report displays the top ten most denied rules for each device you have selected for the report. This report returns the top 10 results for every device selected for the report. If you selected 5 devices, the report returns 50 results. **Note:** Shadowed rule reports are only capable of displaying one report per device.

Table 28. Device Rules Chart parameters (continued)

Parameter	Description
Devices	Select the devices included in the report. The options include: **All Devices** - Select this option to include all devices in QRadar Risk Manager in your report. **Adapter** - From the list, select an adapter type to include in your report. Only one adapter type can be selected from the list for a report. **Specific Devices** - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report. To add individual devices to your report: 1. Click **Browse** to display the Device Selection window. 2. Select any devices and click **Add Selected**. To add all devices to your report: 1. Click **Browse** to display the Device Selection window. 2. Click **Add All**. To search for devices to include in your report: 1. Click **Browse** to display the Device Selection window. 2. Click **Search**. 3. Select the search options to filter the full device list by configuration obtained, IP or CIDR address, hostname, type, adapter, vendor, or model. 4. Click **Search**. 5. Select any devices and click **Add Selected**.

Device Unused Objects charts

A Device Unused Objects report displays object reference groups that are not being used by your network device.

This report displays object references, such as a collection of IP address, CIDR address ranges, or host names that are unused by your network device.

When you configure a device unused objects container, you configure values for the following parameters:

Table 29. Device Unused Objects report parameters

Parameter	Description
Container Details - Device Unused Objects	
Limit Objects to Top	From the list, select the number of rules to be displayed in the generated report.
Devices	Select the devices included in the report. The options include: **All Devices** - Select this option to include all devices in IBM Security QRadar Risk Manager in your report. **Adapter** - From the list, select an adapter type to include in your report. Only one adapter type can be selected from the list for a report. **Specific Devices** - Select this option to only include specific devices in your report. The Device Selection window allows you to select and add devices to your report. To add individual devices to your report: 1. Click **Browse** to display the Device Selection window. 2. Select any devices and click **Add Selected**. To add all devices to your report: 1. Click **Browse** to display the Device Selection window. 2. Click **Add All**. To search for devices to include in your report: 1. Click **Browse** to display the Device Selection window. 2. Click **Search**. 3. Select the search options to filter the full device list by configuration obtained, IP or CIDR address, hostname, type, adapter, vendor, or model. 4. Click **Search**. 5. Select any devices and click **Add Selected**.

Chapter 12. Policy Management

You use the IBM Security QRadar Risk Manager Policy Management pages to view details about policy compliance and policy risk changes for assets, policies, and policy checks.

The QRadar Risk Manager Policy Management pages display data from the last run policy. You can filter the data by asset, by policy or by policy check.

Policy management use cases

Use the Policy Management pages with **Risk** dashboard items to find out more information about assets and policies that failed compliance.

- The **By Asset** page includes information and links to the policies that the assets failed.
- The **By Policy** page includes information about the number and percentage of assets that passed or failed and, if relevant, a link to the policy checks the policy uses.
- The **By Policy Check** page includes information about the number and percentages of assets that pass or fail individual policy checks.

Use the Policy Management pages with **Risk Change** dashboard items to investigate policies and policy checks that display increases in risk. The **Risk Change** dashboard item contains links to the **By Policy** and **By Policy Checks** pages.

For more information about the **Risk** and **Risk Change** dashboard items, see the *IBM Security QRadar SIEM Users Guide*.

Chapter 13. Use simulations in IBM Security QRadar Risk Manager

Use simulations to define, schedule, and run exploit simulations on your network. You can create, view, edit, duplicate, and delete simulations.

You can create simulations that are based on a series of rules that can be combined and configured. The simulation can be scheduled to run on a periodic basis or run manually. After a simulation is complete, you can review the results of the simulation and approve any acceptable or low risk result that is based on your network policy. When you review results you can approve acceptable actions or traffic from your results. After you tune your simulation, you can configure the simulation to monitor the results.

When you monitor a simulation, you can define how you want the system to respond when unapproved results are returned. A system response can be an email, the creation of an event, or to send the response to syslog.

Simulations can be modeled off of a current topology or a topology model.

The Simulation page summarizes information about simulations and simulation results.

Simulation results display only after a simulation is complete. After a simulation is complete, the **Results** column lists the dates and the corresponding results of your simulation.

Simulations

View the simulations that are created by users and the simulation results on the simulations page.

The Simulations window provides the following information:

Table 30. Simulation definitions parameters

Parameter	Description
Simulation Name	The name of the simulation, as defined by the creator of the simulation.
Model	The model type. Simulations can be modeled from the current topology or another topology model. The options are: • Current Topology • The name of the topology model
Groups	The groups that the simulation is associated with.
Created By	The user who created the simulation.
Creation Date	The date and time that the simulation was created.
Last Modified	The date and time that the simulation was last modified.

Table 30. Simulation definitions parameters (continued)

Parameter	Description
Schedule	The frequency the simulation is scheduled to run. The options include: **Manual** - The simulation runs when it is manually executed. **Once** - Specify the date and time the simulation is scheduled to run. **Daily** - Specify the time of day the simulation is scheduled to run. **Weekly** - Specify the day of the week and the time the simulation is scheduled to run. **Monthly** - Specify the day of the month and time the simulation is scheduled to run.
Last Run	The last date and time that the simulation was run.
Next Run	The date and time that the next simulation will be run.
Results	If the simulation is run, this parameter includes a list of dates for the results of your simulations. You can select a date and view the results.

Creating a simulation

You can create simulations that are based on a series of rules that can be combined and configured.

About this task

Parameters that can be configured for simulation tests are underlined. The following table describes the simulation tests that you can configure.

Table 31. Simulation tests

Test Name	Description	Parameters
Attack targets one of the following IP addresses	Simulates attacks against specific IP addresses or CIDR ranges.	Configure the IP addresses parameter to specify the IP address or CIDR ranges to which you want this simulation to apply.
Attack targets one of the following networks	Simulates attacks targeting networks that are a member of one or more defined network locations.	Configure the networks parameter to specify the networks to which you want this simulation to apply.
Attack targets one of the following asset building blocks	Simulates attacks that target one or more defined asset building blocks.	Configure the asset building blocks parameters to specify the asset building blocks to which you want this simulation to apply.

Table 31. Simulation tests (continued)

Test Name	Description	Parameters
Attack targets one of the following reference sets	Simulates attacks that target one or defined reference sets.	Configure the reference sets parameters to specify the reference sets to which you want this simulation to apply.
Attack targets a vulnerability on one of the following ports using protocols	Simulates attacks that target a vulnerability on one or more defined ports.	Configure the following parameters: Open Ports - Specify the ports that you want this simulation to consider. Protocols - Specify the protocol that you want this simulation to consider.
Attack targets assets susceptible to one of the following vulnerabilities	Simulates attacks that target assets that are susceptible to one or more defined vulnerabilities.	Configure the **vulnerabilities** parameter to identify the vulnerabilities that want this test to apply. You can search for vulnerabilities in OSVDB ID, Bugtraq ID, CVE ID, or title.
Attack targets assets susceptible to vulnerabilities with one of the following classifications	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities for one or more defined classifications.	Configure the **classifications** parameter to identify the vulnerability classifications. For example, a vulnerability classification might be Input Manipulation or Denial of Service.
Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5	A Common Vulnerability Scoring System (CVSS) value is an industry standard for assessing the severity of vulnerabilities. This simulation filters assets in your network that include the configured CVSS value. Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities with a CVSS score greater than 5.	Click **Greater Than 5**, and then select an operator. The default operator is greater than **5**

Table 31. Simulation tests (continued)

Test Name	Description	Parameters
Attack targets assets susceptible to vulnerabilities disclosed after this date	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities discovered before, after, or on the configured date.	Configure the following parameters: **before** | **after** | **on** - Specify whether you want the simulation to consider the disclosed vulnerabilities to be after, before, or on the configured date on assets. The default is before. **this date** - Specify the date that you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more text entry.	Configure the **text entries** parameter to identify the asset name, vendor, version, or service you want this simulation to consider.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Allows you to simulate attacks targeting an asset that is susceptible to vulnerabilities matching the asset name, vendor, version or service based one or more regular expression.	Configure the **regular expressions** parameter to identify the asset name, vendor, version, or service you want this simulation to consider.

The following contributing tests are deprecated and hidden in the Policy Monitor:

- **attack targets a vulnerability on one of the following operating systems**
- **attack targets assets susceptible to vulnerabilities from one of the following vendors**
- **attack targets assets susceptible to vulnerabilities from one of the following products**

The deprecated contributing tests are replaced by other tests.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. From the **Actions menu**, select **New**.
4. Type a name for the simulation in the **What do you want to name this simulation** parameter.
5. From the **Which model do you want to base this on** drop-down list, select the type of data you want to return. All existing topology models are listed. If you select **Current Topology**, then the simulation uses the current topology model.
6. Choose one of the following options:

Option	Description
Select Use Connection Data	The simulation is based on connection and topology data.
Clear Use Connection Data	The simulation is only based on topology data. If your topology model does not include any data and you clear the **Use Connection Data** check box, the simulation does not return any results.

7. From the **Importance Factor** list, select the level of importance you want to associate with this simulation.

   The Importance Factor is used to calculate the Risk Score. The range is 1 (low importance) to 10 (high importance). The default is 5.

8. From the **Where do you want the simulation to begin** list, select an origin for the simulation.

   The chosen value determines the start point of the simulation. For example, the attack originates at a specific network. The selected simulation parameters are displayed in the **Generate a simulation where** window.

9. Add simulation attack targets to the simulation test.

10. Using the **Which simulations do you want to include in the attack field**, select the **+** sign beside the simulation you want to include.

    The simulation options are displayed in the **Generate a simulation where** window.

11. From the **Generate a simulation where** window, click any underlined parameters to further configure simulation parameters.

12. In the **Run this simulation for** menu, select the number of steps you want to run this simulation (1 - 5).

13. In the steps menu, choose the schedule for running the simulation.

14. In the groups area, select a check box for any group you want to assign this simulation.

15. Click **Save Simulation**.

Editing a simulation

You can edit simulations.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the simulation definition you want to edit.
4. From the **Actions** menu, select **Edit**.
5. Update parameters, as necessary.

   For more information about the Simulation parameters, see Simulation tests.

6. Click **Save Simulation**.

Duplicating a simulation

You can duplicate simulations.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the simulation you want to duplicate.
4. From the **Actions** menu, select **Duplicate**.
5. Type the name for the simulation.
6. Click **OK**.

Deleting a simulation

You can delete simulations.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the simulation you want to delete.
4. From the **Actions** menu, select **Delete**.
5. Click **OK**.

Manually running a simulation

Use the Simulation Editor to manually run a simulation.

Procedure

1. Click the **Risks** tab.
2. From the **Actions** menu, select **Run Simulation**.
3. Click **OK**.

Results

The simulation process can take an extended period of time. While the simulation is running, the Next Run column indicates the percentage complete. When complete, the Results column displays the simulation date and time.

If you run a simulation and then perform changes that affect the tests associated with the simulation, these changes might take up to an hour to display.

Managing simulation results

After a simulation runs, the Results column displays a drop-down list containing a list of the dates when the simulation was generated.

Simulation results are retained for 30 days. Results only display in the Results column after a simulation runs.

Viewing simulation results

You can view simulation results in the Results column of the Simulations page.

About this task

Results only display in the Results column after a simulation runs. Simulation results provide information on each step of the simulation.

For example, the first step of a simulation provides a list of the directly connected assets that are affected by the simulation. The second step lists assets in your network that can communicate to first-level assets in your simulation.

When you click View Result, the following information is provided:

Table 32. Simulation result information

Parameter	Description
Simulation Definition	The description of the simulation.
Using Model	The name of the model against which the simulation was run.
Simulation Result	The date on which the simulation was run.
Step Results	The number of steps for the result that includes the step that is being displayed.
Assets Compromised	The total number of assets that are compromised in this step and across all simulation steps. If the topology model includes data from an IP range of /32 defined as reachable, then IBM Security QRadar Risk Manager does not validate those assets against the database. Therefore, those assets are not considered in the Asset Compromised total. QRadar Risk Manager only validates assets in broader IP ranges, such as /24 to determine which assets exist.
Risk Score	Risk score is a calculated value based on the number of results, steps, the number of compromised assets, and the importance factor that is assigned to the simulation. This value indicates the severity level that is associated with the simulation for the displayed step.

You can move your mouse pointer over a connection to determine the list of assets that are affected by this simulation.

The top 10 assets display when you move your mouse over the connection.

Move your mouse pointer over the connection to highlight the path through the network, as defined by the subnet.

The simulation result page provides a table called, Results for this step. This table provides the following information:

Table 33. Results for this step information

Parameter	Description
Approve	Allows you to approve simulation results. See Approving simulation results.
Parent	The originating IP address for the displayed step of the simulation.
IP	The IP address of the affected asset.

Table 33. Results for this step information (continued)

Parameter	Description
Network	The network of the target IP addresses, as defined in the network hierarchy.
Asset Name	The name of the affected asset, as defined by the asset profile.
Asset Weight	The weight of the affected asset, as defined in the asset profile.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the Results column, select the date and time of the simulation you want to view using the list.
4. Click **View Result**. You can view the simulation result information, starting at step 1 of the simulation.
5. View the Results for this Step table to determine the assets that are affected.
6. To view the next step of the simulation results, click **Next Step**.

Approving simulation results

You can approve simulation results.

About this task

You might approve network traffic that is deemed low risk or normal communication on the asset. When you approve results, you filter the result list so that future simulations ignore normal or approved communications.

Results only display in the **Results** column after a simulation runs.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the Results column, select the date and time of the simulation that you want to view by using the list.
4. Click **View Result**.
5. In the Results for this step table, use one of the following methods to approve assets:

Option	Description
Approve Selected	Select the check box for each asset that you want to approve, and then click **Approve Selected.**
Approve All	Click to approve all assets that are listed.

6. Optional. Click **View Approved** to view all approved assets.

Revoking simulation approval

You can take an approved connection or communication off of the approved list. After an approved simulation result is removed, future simulations display non-approved communications in the simulation results.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. In the Results column, select the date and time of the simulation you want to view using the list.
4. **View Result**.
5. Click **View Approved** to view all approved assets.
6. Choose one of the following options:

Option	Description
Revoke Selected	Select the check box for each asset that you want to revoke, and then click **Revoke Selected.**
Revoke All	Click to revoke all assets listed.

Monitoring simulations

You can monitor a simulation to determine if the results of the simulation changed. If a change occurs, then an event is generated. A maximum of 10 simulations can be in monitor mode.

About this task

When a simulation is in monitor mode, the defaults time range is 1 hour. This value overrides the configured time value when the simulation was created.

For information about event categories, see the *IBM Security QRadar SIEM Users Guide*.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the simulation that you want to monitor.
4. Click **Monitor**.
5. In the **Event Name** field, type the name of the event you want to display on the **Log Activity** and **Offenses** tab.
6. In the **Event Description** field, type a description for the event. The description is displayed in the Annotations of the event details.
7. From the **High-Level Category** list, select the high-level event category that you want this simulation to use when processing events.
8. From the **Low-Level Category** list, select the low-level event category that you want this simulation to use when processing events.
9. Select the **Ensure the dispatched event is part of an offense** check box if you want, as a result of this monitored simulation, the events that are forwarded to the Magistrate component. If no offense was generated, then a new offense

is created. If an offense exists, this event is added to the existing offense. If you select the check box, then choose one of the following options:

Option	Description
Question/Simulation	All events from a question are associated with a single offense.
Asset	A unique offense is created (or updated) for each unique asset.

10. In the **Additional Actions** section, select one or more of the following options:

Option	Description
Email	Select this check box and specify the email address to send notifications if the event is generated. Use a comma to separate multiple email addresses.

Send to Syslog	Select this check box if you want to log the event.
	
	For example, the syslog output might resemble:
	
	`Sep 28 12:39:01 localhost.localdomain ECS:`
	`Rule 'Name of Rule'Fired: 172.16.60.219:12642 ->`
	`172.16.210.126:6666 6, Event Name:SCAN SYN FIN,`
	`QID: 1000398, Category: 1011, Notes: Eventdescription`

Notify	Select this check box if you want events that generate as a result of this monitored question to display in the System Notifications item in the Dashboard.

11. In the **Enable Monitor** section, select the check box to monitor the simulation.
12. Click **Save Monitor**.

Grouping simulations

Assigning simulations to groups is an efficient way to view and track all simulations. For example, you can view all simulations that are related to compliance.

About this task

As you create new simulations, you can assign the simulations to an existing group.

After you create a group, you can drag groups in the menu tree to change the organization.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the group under which you want to create a new group.
5. Click **New**.
6. In the **Name** field, type a name for the new group. The group name can be up to 255 characters in length.

7. In the **Description field,** type a description for the group. The description can be up to 255 characters in length.
8. Click **OK**.

Editing a group

You can edit a group.

About this task

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the group you want to edit.
5. Click **Edit**.
6. Update information in the Name and Description fields as required.
7. Click **OK**.

Copying an item to another group

Using the groups functionality, you can copy a simulation to one or many groups.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the question you want to copy to another group.
5. Click **Copy**.
6. Select the check box for the group to which you want to copy the simulation.
7. Click **Copy**.

Deleting an item from a group

You can delete an item from a group.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the top level group.
5. From the list of groups, select the item or group you want to delete.
6. Click **Remove**.
7. Click **OK**.

Assigning an item to a group

You can assign a simulation to a group.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.

3. Select the simulation you want to assign to a group.
4. Using the **Actions** menu, select **Assign Groups**.
5. Select the group to which you want the question assigned.
6. Click **Assign Groups**.

Chapter 14. Topology models

You can use a topology model to define virtual network models based on your existing network.

You can create a network model based on a series of modifications that can be combined and configured. This allows you to determine the effect of configuration changes on your network using a simulation. For more information about simulations, see Using simulations.

You can view topology models on the Simulations page. Topology models provides the following information:

Table 34. Model definitions parameters

Parameter	Description
Model Name	The name of the topology model, as defined by the user when created.
Group(s)	The groups to which this topology is associated.
Created By	The user who created the model definition.
Created On	The date and time that the model definition was created.
Last Modified	The number of days since the model definition was created.

Creating a topology model

You can create one or more topology models.

About this task

The following table describes the test names and parameters that you can configure.

Table 35. Topology tests

Test Name	Parameters
A rule is added to the selected devices that allows connections from source CIDRs to destination CIDRs on protocols, ports	Configure the following parameters: **devices** - Specify the devices to which you want to add to this rule. In the Customize Parameter window, select the All check box to include all devices or you can search devices using one of the following search criteria: **IP/CIDR** - Select the IP/CIDR option and specify the IP address or CIDR that you want to add to this rule to. **Hostname** - Select the Hostname option and specify the hostname you want to filter. To search for multiple hostnames, use a wildcard character (*) at the beginning or end of the string. **Adapter** - Select the Adapter option and use the drop-down list to filter the device list by adapter. **Vendor** - Select the Vendor option and use the drop-down list to filter the device list by vendor. You can also specify a model for the vendor. To search for multiple models, use a wildcard character (*) at the beginning or end of the string. **allows** | **denies** - Select the condition (accept or denied) for connections that you want this test to apply. **CIDRs** - Select any source IP addresses or CIDR ranges that you want to add to this rule to. **CIDRs** - Select any destination IP addresses or CIDR ranges that you want to add to this rule to. **protocols** - Specify the protocols that you want to add to this rule to. To include all protocols, select the All check box. **ports** - Specify the ports that you want to add to this rule to. To include all ports, select the All check box.

Table 35. Topology tests (continued)

Test Name	Parameters
A rule is added to the selected IPS devices that allows connections from source CIDRs to destination CIDRs with vulnerabilities	Configure the following parameters: **IPS devices** - Specify the IPS devices that you want this topology model to include. To include all IPS devices, select the All check box. allows │ denies - Specify the condition (accept or denied) for connections that you want this test to apply. **CIDRs** - Specify any source IP addresses or CIDR ranges that you want this topology model to include. **CIDRs** - Specify any destination IP addresses or CIDR ranges that you want this topology model to include. **vulnerabilities** - Specify the vulnerabilities that you want to apply to the topology model. You can search for vulnerabilities using the Bugtraq ID, OSVDB ID, CVE ID, or title.
The following assets allow connections to the selected ports	Configure the following parameters: assets - Specify the assets that you want this topology model to include. **allow** │ deny - Specify the condition (allow or deny) for connections that you want this topology model to apply. The default is allow. ports - Specify the ports that you want this topology model to include. To include all ports, select the All check box.
Assets in the following asset building blocks allow connections to ports	Configure the following parameters: assets building blocks - Specify the building blocks that you want this topology model to include. **allow** │ deny - Specify the condition (allow or deny) that you want this topology model to apply. The default is allow. **ports** - Specify the ports that you want this topology model to include. To include all ports, select the All check box.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**

3. From the **Actions** menu, select New.
4. In the **What do you want to name this model** field, type a name for the model definition.
5. In the **Which modifications do you want to apply to your model** pane, select the modifications that you want to apply to the topology to create your model.
6. Configure the tests added to the **Configure model as follows** pane.
7. When the test is displayed in the pane, the configurable parameters are underlined. Click each parameter to further configure this modification for your model. In the groups area, select the check box to assign groups to this question.
8. Click **Save Model.**

Editing a topology model

You can edit a topology model.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Select the model definition you want to edit.
4. From the **Actions** menu, select Edit.
5. Update parameters, as necessary.

   For more information about the Model Editor parameters, see Creating a topology model.
6. Click **Save Model**.

Duplicating a topology model

You can duplicate a topology model.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Select the model definition you want to duplicate.
4. From the **Actions** menu, select **Duplicate**.
5. Type a name that you want to assign to the copied topology model.
6. Click **OK**.
7. Edit the model.

Deleting a topology model

You can delete a topology model.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Select the model definition you want to delete.
4. From the **Actions** menu, select **Delete**.
5. Click **OK**.

Group topology models

You can group and view your topology models based on your chosen criteria.

Categorizing your topology model is an efficient way to view and track your models. For example, you can view all topology models related to compliance.

As you create new topology models, you can assign the topology models to an existing group. For information on assigning a group, see Creating a topology model.

Viewing groups

You can view topology models using groups.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Using the **Group** list, select the group you want to view.

Creating a group

You can create a group to efficiently view and track topology models.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Click **Groups**.
4. From the menu tree, select the group under which you want to create a new group.

   After you create the group, you can drag and drop groups in the menu tree items to change the organization.
5. Click **New**.
6. Type the name that you want to assign to the new group. The name can be up to 255 characters in length.
7. Type a description for the group. The description can be up to 255 characters in length.
8. Click **OK**.
9. If you want to change the location of the new group, click the new group and drag the folder to location in your menu tree.

Editing a group

You can edit a group.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Topology Models**.
3. Click **Groups**.
4. From the menu tree, select the group you want to edit.
5. Click **Edit**.
6. Update values for the parameters

7. Click **OK**.
8. If you want to change the location of the group, click the new group and drag the folder to location in your menu tree.

Copying an item to another group

Using the groups functionality, you can copy a topology model to one or many groups.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulations** > **Topology Models**.
3. Click **Groups**.
4. From the menu tree, select the question you want to copy to another group.
5. Click **Copy**.
6. Select the check box for the group to which you want to copy the simulation.
7. Click **Copy**.

Deleting an item from a group

You can delete an item from a group.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Click **Groups**.
4. From the menu tree, select the top level group.
5. From the list of groups, select the item or group you want to delete.
6. Click **Remove**.
7. Click **OK**.

Assign a topology to a group

You can assign a topology model to a group.

Procedure

1. Click the **Risks** tab.
2. On the navigation menu, select **Simulation** > **Simulations**.
3. Select the topology model you want to assign to a group.
4. From the **Actions** menu, select **Assign Group**.
5. Select the group to which you want the question assigned.
6. Click **Assign Groups**.

Chapter 15. Audit log data

Changes made by IBM Security QRadar Risk Manager users are recorded in the **Log Activity** tab of IBM Security QRadar SIEM.

All logs display in the Risk Manager Audit category. For more information about using the **Log Activity** tab in QRadar SIEM, see the *IBM Security QRadar SIEM Users Guide*.

Logged actions

Actions are logged for components.

The following table lists the categories and corresponding actions that are logged.

Table 36. Logged actions

Category	Action
Policy Monitor	Create a question.
	Edit a question.
	Delete a question.
	Submit a question manually.
	Submit a question automatically.
	Approve results.
	Revoke results approval.
Topology Model	Create a topology model.
	Edit a topology model.
	Delete a topology model.
Topology	Save layout.
	Create a topology saved search.
	Edit a topology saved search
	Delete a topology saved search
	Placing an IPS.
Configuration Monitor	Create a log source mapping
	Edit a log source mapping
	Delete a log source mapping
Simulations	Create a simulation.
	Edit a simulation.
	Delete a simulation.
	Manually run a simulation.
	Automatically run a simulation.
	Approve simulation results.
	Revoke simulation results.

Table 36. Logged actions (continued)

Category	Action
Configuration Source Management	Successfully authenticate for the first time on a session.
	Add a device.
	Remove a device.
	Edit the IP address or adapter for a device.
	Save a credential configuration.
	Delete a credential configuration.
	Save a protocol configuration.
	Remove a protocol configuration.
	Create a schedule for a backup job.
	Delete a schedule for a backup job.
	Edit a backup job.
	Add a backup job.
	Delete a backup job.
	Run a scheduled backup job.
	Complete a scheduled job whether the job is successful or has failed.
	After a backup job has completed processing and the configuration was persisted, no changes discovered.
	After a backup job has completed processing and the configuration was persisted, changes were discovered.
	After a backup job has completed processing and the configuration was persisted, unpersisted changes were discovered.
	After a backup job has completed processing and the configuration that was previously persisted no longer resides on the device.
	Adapter operation attempt has begun, which includes protocols and credentials.
	Adapter operation attempt has been successful, including the protocols and credentials.

Viewing user activity

You can view user activity for IBM Security QRadar Risk Manager users.

Procedure

1. Click the **Log Activity** tab. If you previously saved a search as the default, the results for that saved search is displayed.
2. Click **Search** > **New Search** to create a search.
3. In the **Time Range** pane, select an option for the time range you want to capture for this search.
4. In the **Search Parameters** pane, define your search criteria:

a. From the first list, select **Category**.

b. From the **High Level Category** drop-down list, select **Risk Manager Audit**.

c. Optional. From the **Low Level Category** drop-down list, select a category to refine your search.

5. Click **Add Filter**.

6. Click **Filter** to search for QRadar Risk Manager events.

Viewing the log file

Audit logs, which are stored in plain text, are archived and compressed when the audit log file reaches a size of 200 MB.

About this task

The current log file is named audit.log. If the audit log file reaches a size of 200 MB a second time, the file is compressed and the old audit log is renamed as audit.1.gz. The file number increments each time a log file is archived. IBM Security QRadar Risk Manager can store up to 50 archived log files.

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>
```

The following table describes the parameters used in the log file.

Table 37. Audit log file information

Parameter	Description
<date_time>	The date and time of the activity in the format: Month Date HH:MM:SS.
<host name>	The host name of the Console where this activity was logged.
<user>	The name of the user that performed the action.
<IP address>	The IP address of the user that performed the action.
(thread ID)	The identifier of the Java™ thread that logged this activity.
<category>	The high-level category of this activity.
<sub-category>	The low-level category of this activity.
<action>	The activity that occurred.
<payload>	The complete record that has changed, if any.

Procedure

1. Using SSH, log in to your IBM Security QRadar SIEM Console as the root user.

2. Using SSH from the IBM Security QRadar SIEM Console, log in to the QRadar Risk Manager appliance as a root user.

3. Go to the following directory: `/var/log/audit`
4. Open your audit log file.

Log file details

Administrators use IBM Security QRadar Risk Manager log files to view user activity and to troubleshoot system issues.

The following table describes the location and content of QRadar Risk Manager log files.

Table 38. QRadar Risk Manager log files

Log file name	Location	Description
`audit.log`	`/var/log/audit/`	Contains the current audit information.
`audit.<1-50>.gz`	`/var/log/audit/`	Contains archived audit information. When the `audit.log` file reaches 200 MB in size, it is compressed and renamed to `audit.1.gz`. The file number increments each time a log file is archived. QRadar Risk Manager can store up to 50 archived log files.
`qradar.log`	`/var/log/`	Contains all process information that is logged by the QRadar Risk Manager server.
`qradar.error`	`/var/log/`	All exceptions and `System.out` and `System.err` messages that are generated by the QRadar Risk Manager server are logged in this file.

Notices

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

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

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

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

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

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

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

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

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines 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 www.ibm.com/legal/copytrade.shtml.

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.

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Glossary

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

The following cross-references are used in this glossary:

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

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

A

adapter
An intermediary software component that allows two other software components to communicate with one another.

asset A manageable object that is either deployed or intended to be deployed in an operational environment.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system.

attack path
The source, destination, and devices associated with an attack.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

C

connection graph
A graph that shows connections from remote network nodes and local IP addresses to local network nodes.

connection line
A line on the connection graph between a remote network node and a local network node or between two local network nodes.

contributing test
A test that examines the risk indicators that are specified in a question.

M

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

NAT See Network Address Translation.

NAT indicator
An indicator on the topology graph that shows that the path between two network connections contains either source or destination address translations.

neighbor data
Data collected from adapters that is used to discover information about devices that are connected to QRadar Quality Manager managed hosts.

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

R

restrictive test
A test that filters the results returned by a contributing test question.

risk indicator
A measure of the potential exposure of a system to a security breach.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

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

S

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

T

time series chart
A graphical representation of network connections over time.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

Index

A

actual communication 79
  contributing questions 76
add asset 60
Address set 14
asset compliance question 41, 43, 66, 67
asset profile 60
asset profiles 64
asset question 39
Asset results 45
assets tab 60
audit log
  actions 145
audit log data 145

B

back up information 23
backup configuration information 22
backup job 24, 25, 27
backup job renaming 26
backup log 23
Backup Log Viewer 23
backup status 23
browser mode
  Internet Explorer web browser 6

C

charts
  configuring 115
  connections 115
  Device Rules 117
  Device Unused Objects 122
CheckPoint SmartConsole
  rule counting 69
compliance 42, 65
compliance benchmarks 42, 65
configuration 9
configuration monitor 3
configuration source management 13
connection graph 91
connections 3, 87, 100
  searching 94
CPSMS 71
creating
  benchmark scan profiles 66
credential set 14
credentials 13
  configuring 14

D

default log in information 6
deprecated contributing questions 79
Deprecated contributing test
  questions 84
device
  adding 18

device *(continued)*
  deleting 19
  importing 17
device configuration 21
  comparing 104
device discovery 16
device groups
  grouping devices 35
device import, CSV file 17
device list
  filtering 20
device results 48
device rules filtering 107
Device/rules test questions 86
devices 18
  adding 19
devices/rules question 40
discovery schedule 30
document mode
  Internet Explorer web browser 6
dynamic routing 7

E

edit asset 60
email server 9
export 43
exporting 100

F

firewall access 9

G

glossary 153
graph 90, 91, 93
graphs 89

H

high availability (HA) 7
high risk vulnerabilities
  prioritizing 57

I

import 43
importance factor 38
introduction vii
Intrusion Prevention System 34
  removing 34
IPS 34
IPv6 7

L

layout 35
log data 145
log file 147, 148
log in information 6
log locations 148
log source mapping 101
  creating 101

M

monitor mode 43, 52, 67
monitor questions 43, 52, 67

N

NAT indicators 33
neighbor data
  collecting 22
network administrator vii
network connections
  monitor 3
network device configuration
  investigating 103
Network group 14
new features
  version 7.2.6 user guide overview 1
non-contiguous network masks 7

P

password 6, 10
policy monitor 4, 37
  assign items to groups 54
  delete item from question group 54,
   137, 144
  managing questions 37
  results for questions 51
  use cases 55
policy monitor questions 43, 75
  creating a group 53
  editing 53
  evaluating results 50
  exporting 44
  grouping 53
  importing 44
  viewing groups 53
policy monitor use case
  actual communication for DMZ 58
  device test communication for Internet
   access 56
  possible communication on protected
   assets 55
possible communication tests
  contributing questions 81
  restrictive tests 84
protocols 27, 28

IBM ®

Printed in USA