IBM Security QRadar
Version 7.2.1

Installation Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 37.

Contents

Introduction to QRadar software installations

IBM® Security QRadar® appliances are preinstalled with software and the Red Hat Enterprise Linux operating system. You can also install QRadar software on your own hardware.

Information about installing IBM Security QRadar software applies to IBM Security QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection products.

To install or recover a high-availability (HA) system, see the *IBM Security QRadar High Availability Guide*.

Intended audience

Network administrators who are responsible for installing and configuring QRadar systems must be familiar with network security concepts and the Linux operating system.

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. QRadar deployment overview

You can install IBM Security QRadar components on a single server for small enterprises, or across multiple servers for large enterprise environments.

For maximum performance and scalability, you must install redundant appliances for each system that requires HA protection. For more information about installing or recovering an HA system, see the *IBM Security QRadar High Availability Guide*.

Activation keys and license keys

When you install IBM Security QRadar products, you must type an activation key. After you install, you must apply your license keys. To avoid typing the wrong key in the installation process, it is important to understand the difference between the keys.

Activation key

The activation key is a 24-digit, 4-part, alphanumeric string that you receive from IBM. All installations of QRadar products use the same software. However, the activation key specifies which software modules to apply for each appliance type. For example, use the IBM Security QRadar QFlow Collector activation key to install only the QRadar QFlow Collector modules.

You can obtain the activation key from the following locations:

- If you purchased an appliance that is preinstalled with QRadar software, the activation key is included on the enclosed CD.
- If you purchased QRadar software or virtual appliance download, a list of activation keys is included in the *Getting Started* document. The *Getting Started* is attached to the confirmation email.

License key

Your system includes a default license key that provides you with access to QRadar software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

The following table describes the restrictions for the default license key:

Table 1. Restrictions for the default license key for QRadar SIEM and QRadar Network Anomaly Detection installations

Usage	Limit
Active log source limit	750
Events per second threshold	5000
Flows per interval	200000
User limit	10
Network object limit	300

Table 2. Restrictions for the default license key for QRadar Log Manager installations

Usage	Limit
Active log source limit	750
Events per second threshold	5000

Table 2. Restrictions for the default license key for QRadar Log Manager installations (continued)

Usage	Limit
User limit	10
Network object limit	300

When you purchase a QRadar product, an email that contains your permanent license keys is sent from IBM. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your default license expires.

Integrated Management Module

Use Integrated Management Module, which is on the back panel of each appliance type, to manage the serial and Ethernet connectors.

You can configure the Integrated Management Module to share an Ethernet port with the IBM Security QRadar product management interface. However, to reduce the risk of losing the connection when the appliance is restarted, configure Integrated Management Module in dedicated mode.

To configure Integrated Management Module, you must access the system BIOS settings by pressing F1 when the IBM splash screen is displayed. For more information about configuring the Integrated Management Module, see the *Integrated Management Module User's Guide* on the CD that is shipped with your appliance.

QRadar components

IBM Security QRadar consolidates event data from log sources that are used by devices and applications in your network.

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

QRadar deployments can include the following components:

QRadar QFlow Collector
Passively collects traffic flows from your network through span ports or network taps. The IBM Security QRadar QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow.

You can install a QRadar QFlow Collector on your own hardware or use one of the QRadar QFlow Collector appliances.

Restriction: The component is available only for QRadar SIEM and QRadar Network Anomaly Detection deployments.

QRadar Console
Provides the QRadar product user interface. The interface delivers real-time event and flow views, reports, offenses, asset information, and administrative functions.

In distributed QRadar deployments, use the QRadar Console to manage hosts that include other components.

QRadar Event Collector
Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component examines the event from the log source and maps the event to a QRadar Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.

QRadar Event Processor
Processes events that are collected from one or more Event Collector components. The Event Processor correlates the information from QRadar products and distributes the information to the appropriate area, depending on the type of event.

The Event Processor also includes information that is gathered by QRadar products to indicate behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

Magistrate
Provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events.

The Magistrate component processes events against the custom rules. If an event matches a rule, the Magistrate component generates the response that is configured in the custom rule.

For example, the custom rule might indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate component uses default rules to process the event. An offense is an alert that is processed by using multiple inputs, individual events, and events that are combined with analyzed behavior and vulnerabilities. The Magistrate component prioritizes the offenses and assigns a magnitude value that is based on several factors, including number of events, severity, relevance, and credibility.

For more information about each component, see the *Administration Guide*.

Prerequisite hardware accessories and desktop software for QRadar installations

Before you install IBM Security QRadar products, ensure that you have access to the required hardware accessories and desktop software.

Desktop software requirements

Ensure that following applications are installed on all desktop systems that you use to access the QRadar product user interface:

- Java™ Runtime Environment (JRE) version 1.7
- Adobe Flash version 10.x

Hardware accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console

- Uninterrupted Power Supply (UPS) for all systems that store data, such as QRadar Console, Event Processor components, or QRadar QFlow Collector components
- Null modem cable if you want to connect the system to a serial console

Important: QRadar products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but does not support software-based RAID installations.

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 tables list the supported versions of web browsers.

Table 3. Supported web browsers for QRadar products

Web browser	Supported version
Mozilla Firefox	• 10.0 Extended Support Release (ESR) • 10.0 Extended Support Release (ESR)
Microsoft Internet Explorer, with document mode and browser mode enabled	• 8.0 • 9.0
Google Chrome	• Latest version

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 **Internet Explorer 7.0 Standards**.

Chapter 2. Installing a QRadar Console or managed host

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

Note: IBM Security QRadar Network Anomaly Detection is a stand-alone appliance. Install QRadar Network Anomaly Detection Console on a QRadar or on your own appliance.

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

Before you begin

Ensure that the following requirements are met:

__ • The required hardware is installed.
__ • For QRadar appliances, a notebook is connected to the serial port on the back of the appliance, or a keyboard and monitor is connected.
__ • You are logged in as the root user.
__ • The activation key is available.

If you use a notebook to connect to the system, you must use a terminal program, such as HyperTerminal. Ensure that you set **Connect Using** option to the appropriate COM port of the serial connector. Ensure that you also set the following properties:

Table 4. Terminal connection properties

Property	Setting
Bits per second	9600
Stop Bits	1
Data bits	8
Parity	None

Procedure

1. If you are using your own appliance, mount the QRadar ISO image
   a. Create the `/media/cdrom` directory by typing the following command:
      `mkdir /media/cdrom`
   b. Obtain the QRadar software.
   c. Mount the QRadar ISO image by typing the following command:
      `mount -o loop` *`path to the QRadar ISO`*`/media/cdrom`
   d. To begin the installation, type the following command:
      `/media/cdrom/setup`
2. For all installations, ensure that the End User License Agreement (EULA) is displayed.

   Tip: Press the Spacebar key to advance through the document.

If you are installing QRadar on your own appliance, you are prompted to continue the installation. This process might take up to several hours.

3. When you are prompted for the activation key, enter the 24-digit, 4-part, alphanumeric string that you received from IBM.

   The letter I and the number 1 (one) are treated the same. The letter O and the number 0 (zero) are also treated the same.

4. For the type of setup, select **normal**.
5. Follow the instructions in the installation wizard to complete the installation.

   The following table contains descriptions and notes to help you configure the installation.

Table 5. Description of network settings

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.
Root password	The password must meet the following criteria: • Contain at least 5 characters • Contain no spaces • Can include the following special characters: @, #, ^, and *.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

6. Apply your license key.
   a. Log in to QRadar:

      `https://`*`IP_Address_QRadar`*

      The default **Username** is `admin`. The **Password** is the password of the root user account.

   b. Click the login.
   c. Click the **Admin** tab.
   d. In the navigation pane, click **System Configuration**.
   e. Click the **System and License Management** icon.
   f. From the **Display** list box, select **Licenses**, and upload you license key.
   g. Select the unallocated license and click **Allocate System to License**.
   h. From the list of licenses, select and license, and click **Allocate License to System**.

Chapter 3. RHEL operating system installations on your own appliance

To ensure a successful installation of IBM Security QRadar on your own appliance, you must install the Red Hat Enterprise Linux operating system.

Ensure that your appliance meets the system requirements for QRadar deployments.

Prerequisites for installing RHEL on your own appliance

Before you install the Red Hat Enterprise Linux (RHEL) operating system on your own appliance, ensure that your system meets the system requirements.

The following table describes the system requirements:

Table 6. System requirements for RHEL installations on your own appliance

Header	**Header**
Supported software version	Version 6.4
Bit version	64-bit
KickStart disks	Not supported
Network Time Protocol (NTP) package	Optional If you want to use NTP as your time server, ensure that you install the NTP package
Memory (RAM) for Console systems	Minimum 8 GB If you enable payload indexing, minimum 24 GB **Important:** You must upgrade your system memory before you install QRadar.
Free disk space for Console systems	Minimum 256 GB **Important:** For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
QRadar QFlow Collector primary drive	Minimum 70 GB
Firewall configuration	WWW (http, https) enabled SSH enabled **Important:** Before you configure the firewall, disable the SELinux option. The QRadar installation includes a default firewall template that you can update in the System Setup window.

Linux partition properties for your own appliance

If you use your own appliance, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Use the values in following table as a guide when you recreate the partitioning on your Red Hat Enterprise Linux operating system.

Table 7. Partition guide for RHEL

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/boot	System boot files	/boot	EXT4	200 MB	Yes	SDA
swap	Used as memory when RAM is full.	empty	swap	Systems with 4 to 8 GB of RAM, the size of the swap partition must match the amount of RAM Systems with 8 to 24 GB of RAM, configure the swap partition size to be 75% of RAM, with a minimum value of 8 GB and a maximum value of 24 GB.	No	SDA
/	Installation area for QRadar, the operating system, and associated files.	/	EXT4	20000 MB If /store mounted on SDB, select **Fill to maximum allowable size**	No	SDA
/store/tmp	Storage area for QRadar temporary files	/store/tmp	EXT4	20000 MB	No	SDA If 2 disks, SDB
/var/log	Storage area for QRadar and system log files	/var/log	EXT4	20000 MB	No	SDA
/store	Storage area for QRadar data and configuration files	/store	XFS	Select the **Fill to maximum allowable size** check box	No	SDA

Restrictions

Future software upgrades might fail if you reformat any of the following partitions or their subpartitions:

- /store
- /store/tmp
- /store/ariel
- /store/ariel/persistent_data

Example: Console partition configurations for multiple disk deployments

For multiple disk deployments only, configure the following partitions for the Console:

Disk 1

boot, swap, OS, QRadar temporary files, and log files

Remaining disks

- RAID5
- Mounted as `/store`
- Stores QRadar data
- Contains FLOWLOGS and DB.

Other QRadar components do not require these storage partitions.

Installing RHEL on your own appliance

You can install the Red Hat Enterprise Linux operating system on your own appliance for use with IBM Security QRadar.

Procedure

1. Copy the Red Hat Enterprise Linux 6.4 operating system DVD ISO to one of the following portable storage devices:
   - Digital Versatile Disk (DVD)
   - Bootable USB flash drive

     For information about creating a bootable USB flash drive, see the *Installing QRadar Using a Bootable USB flash drive* technote on the IBM web site (www.ibm.com/support).
2. Insert the portable storage device into your appliance and restart your appliance.
3. From the starting menu, select one of the following options:
   - Select the `USB` or `DVD` drive as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in `legacy` mode.
4. When prompted, log in to the system as the root user.
5. To prevent an issue with Ethernet interface address naming, on the Welcome page, press the Tab key and at the end of the `Vmlinuz initrd=initrd.image` line add `biosdevname=0`.
6. Follow the instructions in the installation wizard to complete the installation:
   a. Select the **Basic Storage Devices** option.
   b. When you configure the host name, the **Hostname** property can include letters, numbers, and hyphens.
   c. When you configure the network, in the Network Connections window, select **System eth0** and then click **Edit** and select **Connect automatically**.
   d. On the **IPv4 Settings** tab, from the **Method** list, select **Manual**.
   e. In the **DNS servers** field, type a comma-separated list.
   f. Select **Create Custom Layout** option.
   g. Configure `EXT4` for the file system type for the `/`, `/boot`, and `/var/log` partitions.
   h. Reformat the swap partition with a file system type of swap.
   i. Select **Basic Server**.
7. When the installation is complete, click **Reboot**.

What to do next

After installation, if your onboard network interfaces are named anything other than `eth0`, `eth1`, `eth2`, and `eth3`, you must rename the network interfaces.

Related reference:

"Linux partition properties for your own appliance" on page 7
If you use your own appliance, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Chapter 4. Virtual appliance installations for QRadar SIEM and QRadar Log Manager

You can install IBM Security QRadar SIEM and IBM Security QRadar Log Manager on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.

To install a virtual appliance, complete the following tasks in sequence:

__ • Create a virtual machine.

__ • Install QRadar software on the virtual machine.

__ • Add your virtual appliance to the deployment.

Overview of supported virtual appliances

A virtual appliance is a IBM Security QRadar system that consists of QRadar software that is installed on a VMWare ESX virtual machine.

A virtual appliance provides the same visibility and functionality in your virtual network infrastructure that QRadar appliances provide in your physical environment.

After you install your virtual appliances, use the deployment editor to add your virtual appliances to your deployment. For more information on how to connect appliances, see the *Administration Guide*.

The following virtual appliances are available:

QRadar SIEM All-in-One Virtual 3190

This virtual appliance is a QRadar SIEM system that can profile network behavior and identify network security threats. The QRadar SIEM All-in-One Virtual 3190 virtual appliance includes an on-board Event Collector and internal storage for events.

The QRadar SIEM All-in-One Virtual 3190 virtual appliance supports the following items:

- Up to 1,000 network objects
- 200,000 flows per interval, depending on your license
- 5,000 Events Per Second (EPS), depending on your license
- 750 event feeds (additional devices can be added to your licensing)
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- QRadar QFlow Collector and Layer 7 network activity monitoring

To expand the capacity of the QRadar SIEM All-in-One Virtual 3190 beyond the license-based upgrade options, you can add one or more of the QRadar SIEM Event Processor Virtual 1690 or QRadar SIEM Flow Processor Virtual 1790 virtual appliances:

QRadar SIEM Event Processor Virtual 1690

This virtual appliance is a dedicated Event Processor that allows you to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar SIEM Event Processor Virtual 1690 includes an on-board Event Collector, Event Processor, and internal storage for events.

The QRadar SIEM Event Processor Virtual 1690 appliance supports the following items:

- Up to 10,000 events per second
- 2 TB or larger dedicated event storage

The QRadar SIEM Event Processor Virtual 1690 virtual appliance is a distributed Event Processor appliance and requires a connection to any QRadar SIEM 3105 or QRadar SIEM 3124 series appliance.

QRadar SIEM Flow Processor Virtual 1790

This virtual appliance is deployed with any QRadar SIEM 3105 or QRadar SIEM 3124 series appliance. The virtual appliance is used to increase storage and includes an on-board Event Processor, and internal storage.

QRadar SIEM Flow Processor Virtual 1790 appliance supports the following items:

- 600,000 flows per interval depending on traffic types
- 2 TB or larger dedicated flow storage
- 1,000 network objects
- QRadar QFlow Collector and Layer 7 network activity monitoring

You can add QRadar SIEM Flow Processor Virtual 1790 appliances to any QRadar SIEM 3105 or QRadar SIEM 3124 series appliance to increase the storage and performance of your deployment.

QRadar VFlow Collector 1290

This virtual appliance provides the same visibility and functionality in your virtual network infrastructure that a QRadar QFlow Collector offers in your physical environment. The QRadar QFlow Collector virtual appliance analyzes network behavior and provides Layer 7 visibility within your virtual infrastructure. Network visibility is derived from a direct connection to the virtual switch.

The QRadar VFlow Collector 1290 virtual appliance supports a maximum of the following items:

- 10,000 flows per minute
- Three virtual switches, with one additional switch that is designated as the management interface.

The QRadar VFlow Collector 1290 virtual appliance does not support NetFlow.

QRadar Event Collector Virtual 1590

This virtual appliance is a dedicated Event Collector, which is required if you want to enable the store and forward feature. The store and forward feature allows you

to manage schedules that control when to start and stop forwarding events from your dedicated Event Collector appliances to Event Processor components in your deployment.

A dedicated Event Collector does not process events and it does not include an on-board Event Processor.

By default, a dedicated Event Collector continuously forwards events to an Event Processor that you must connect using the deployment editor. The maximum Event Per Second (EPS) is controlled by the Event Processor.

System requirements for virtual appliances

To ensure that IBM Security QRadar works correctly, ensure that virtual appliance that you use meets the minimum software and hardware requirements.

Before you install your virtual appliance, ensure that the following minimum requirements are met:

Table 8. Requirements for virtual appliances

Requirement	Description
VMware client	VMware ESXi Version 5.0 VMware ESXi Version 5.1 For more information about VMWare clients, see the VMware website (www.vmware.com)
Virtual disk size on all appliance except QRadar QFlow Collector appliances	Minimum: 256 GB **Important:** For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
Virtual disk size for QRadar QFlow Collector appliances	Minimum: 70 GB

The following table describes the minimum memory requirements for virtual appliances.

Table 9. Minimum and optional memory requirements for QRadar virtual appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar VFlow Collector 1290	6 GB	6 GB
QRadar Event Collector Virtual 1590	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1690	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1790	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3190	24 GB	48 GB
QRadar Log Manager Virtual 1790	24 GB	48 GB

Creating your virtual machine

To install a virtual appliance, you must first use VMware vSphere Client 5.0 to create a virtual machine.

Procedure

1. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
2. Use the following steps to guide you through the choices:
   a. In the **Configuration** pane of the Create New Virtual Machine window, select **Custom**.
   b. In the **Virtual Machine Version** pane, select **Virtual Machine Version: 7**.
   c. For the **Operating System (OS)**, select **Red Hat Enterprise Linux 6 (64-bit)**.
   d. On the **CPUs** page, configure the number of virtual processors that you want for the virtual machine:

      When you configure the parameters on the **CPU** page, you must configure a minimum of two processors. The combination of number of virtual sockets and number of cores per virtual socket determines how many processors are configured on your system.

      The following table provides examples of **CPU** page settings you can use:

Table 10. Same **CPU** *page settings*

Number of processors	Sample CPU page settings
2	Number of virtual sockets = 1 Number of cores per virtual socket = 2
2	Number of virtual sockets = 2 Number of cores per virtual socket = 1
4	Number of virtual sockets = 4 Number of cores per virtual socket = 1
4	Number of virtual sockets = 2 Number of cores per virtual socket = 2

   e. In the **Memory Size** field, type or select 8 or higher.
   f. Use the following table to configure you network connections.

Table 11. Descriptions for network configuration parameters

Parameter	Description
How many NICs do you want to connect	You must add at least one Network Interface Controller (NIC)
Adapter	`VMXNET3`

   g. In the **SCSI controller** pane, select **VMware Paravirtual**.
   h. In the **Disk** pane, select **Create a new virtual disk** and use the following table to configure the virtual disk parameters.

Table 12. Settings for the virtual disk size and provisioning policy parameters

Property	Option
Capacity	256 or higher (GB)
Disk Provisioning	Thin provision

Table 12. Settings for the virtual disk size and provisioning policy parameters (continued)

Property	Option
Advanced options	Do not configure

3. On the **Ready to Complete** page, review the settings and click **Finish**.

Installing the QRadar software on a virtual machine

After you create your virtual machine, you must install the IBM Security QRadar software on the virtual machine.

Before you begin

Ensure that the activation key is readily available.

Procedure

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. In the **Commands** pane, click **Edit Settings**.
4. In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.
5. In the **Device Status** pane, select the **Connect at power on** check box.
6. In the **Device Type** pane, select **Datastore ISO File** and click **Browse**.
7. In the Browse Datastores window, locate and select the QRadar product ISO file, click **Open** and then click **OK**.
8. After the QRadar product ISO image is installed, right-click your virtual machine and click **Power** > **Power On.**
9. Log in to the virtual machine by typing `root` for the user name.

   The user name is case-sensitive.
10. Ensure that the End User License Agreement (EULA) is displayed.

    Tip: Press the Spacebar key to advance through the document.
11. For the type of setup, select **normal**.
12. For QRadar Console installations, select the **Enterprise** tuning template.
13. Follow the instructions in the installation wizard to complete the installation.

    The following table contains descriptions and notes to help you configure the installation.

Table 13. Description of network settings

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional

Table 13. Description of network settings (continued)

Network Setting	Description
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.
Root password	The password must meet the following criteria: • Contain at least 5 characters • Contain no spaces • Can include the following special characters: @, #, ^, and *.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

Adding your virtual appliance to your deployment

After the IBM Security QRadar software is installed, add your virtual appliance to your deployment.

Procedure

1. Log in to the QRadar Console.
2. On the **Admin** tab, click the **Deployment Editor** icon.
3. In the **Event Components** pane on the **Event View** page, select the virtual appliance component that you want to add.
4. On the first page of the **Adding a New Component** task assistant, type a unique name for the virtual appliance.

   The name that you assign to the virtual appliance can be up to 20 characters in length and can include underscores or hyphens.
5. Complete the steps in the task assistant.
6. From the **Deployment Editor** menu, click **File** > **Save to staging**.
7. On the **Admin** tab menu, click **Deploy Changes**.
8. Apply your license key.
   a. Log in to QRadar:

      `https://`*`IP_Address_QRadar`*

      The default **Username** is `admin`. The **Password** is the password of the root user account.
   b. Click the login.
   c. Click the **Admin** tab.
   d. In the navigation pane, click **System Configuration**.
   e. Click the **System and License Management** icon.
   f. From the **Display** list box, select **Licenses**, and upload you license key.

g. Select the unallocated license and click **Allocate System to License**.
h. From the list of licenses, select and license, and click **Allocate License to System**.

Chapter 5. Installations from the recovery partition

When you install IBM Security QRadar products, the installer (ISO image) is copied to the recovery partition. From this partition, you can reinstall QRadar products. Your system is restored back to the default configuration. Your current configuration and data files are overwritten

When you restart your QRadar appliance, an option to reinstall the software is displayed. If you do not respond to the prompt within 5 seconds, the system continues to start as normal. Your configuration and data files are maintained. If you choose the reinstall option, a warning message is displayed and you must confirm that you want to reinstall.

After a hard disk failure, you might not be able to reinstall from the recovery partition because the recovery partition is no longer be available. If you experience a hard disk failure, contact Customer Support for assistance.

Any software upgrades of QRadar version 7.2.0 replaces the existing ISO file with the newer version.

These guidelines apply to new QRadar version 7.2.0 installations or upgrades from new QRadar version 7.0 installations on QRadar version 7.0 appliances.

Installing from the recovery partition

You can reinstall IBM Security QRadar products from the recovery partition.

Before you begin

Locate your activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM. You can find the activation key in one of the following locations:

- Printed on a sticker and physically placed on your appliance.
- Included with the packing slip; all appliances are listed along with their associated keys.

If you do not have your activation key, go to the IBM Support website (www.ibm.com/support) to obtain your activation key. You must provide the serial number of the QRadar appliance. Software activation keys do not require serial numbers.

If your deployment includes offboard storage solutions, you must disconnect your offboard storage before you reinstall QRadar. After you reinstall, you can remount your external storage solutions. For more information on configuring off-board storage, see the *Offboard Storage Guide*.

Procedure

1. Restart your QRadar appliance and select **Factory re-install**.
2. Type `flatten`.

The installer partitions and reformats the hard disk, installs the OS, and then reinstalls theQRadar product. You must wait for the flatten process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

3. Type `SETUP`.
4. Log in as the root user.
5. Ensure that the End User License Agreement (EULA) is displayed.

   Tip: Press the Spacebar key to advance through the document.
6. For QRadar Console installations, select the **Enterprise** tuning template.
7. Follow the instructions in the installation wizard to complete the installation.

   The following table contains descriptions and notes to help you configure the installation.

Table 14. Description of network settings

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.
Root password	The password must meet the following criteria: • Contain at least 5 characters • Contain no spaces • Can include the following special characters: @, #, ^, and *.

After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

8. Apply your license key.
   a. Log in to QRadar:

      `https://`*`IP_Address_QRadar`*

      The default **Username** is `admin`. The **Password** is the password of the root user account.
   b. Click the login.
   c. Click the **Admin** tab.
   d. In the navigation pane, click **System Configuration**.
   e. Click the **System and License Management** icon.
   f. From the **Display** list box, select **Licenses**, and upload you license key.
   g. Select the unallocated license and click **Allocate System to License**.

h. From the list of licenses, select and license, and click **Allocate License to System**.

Chapter 6. Network settings management

Use the `qchange_netsetup script` to change the network settings of your IBM Security QRadar system. Configurable network settings include host name, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

Changing the network settings in an all-in-one system

You can change the network settings in your all-in-one system. An all-in-one system has all IBM Security QRadar components that are installed on one system.

Before you begin

You must have a local connection to your QRadar Console.

Procedure

1. Log in to as the root user:

   Username: `root`

   Password: *password*
2. Type the following command:

   `qchange_netsetup`
3. Follow the instructions in the wizard to complete the configuration.

   The following table contains descriptions and notes to help you configure the network settings.

Table 15. Description of network settings for an all-in-one QRadar Console

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.

A series of messages are displayed asQRadar processes the requested changes. After the requested changes are processed, the QRadar system is automatically shutdown and restarted.

Changing the network settings of a QRadar Console in a multisystem deployment

To change the network settings in a multi-system IBM Security QRadar deployment, remove all managed hosts, change the network settings, readd the managed hosts, and then reassign the component.

Procedure

1. To remove managed hosts, log in to QRadar:

   `https://IP_Address_QRadar`

   The **Username** is `admin`.

   a. Click the **Admin** tab.

   b. Click the **Deployment Editor** icon.

   c. In the Deployment Editor window, click the **System View** tab.

   d. For each managed host in your deployment, right-click the managed host and select **Remove host**.

   e. On the **Admin** tab, click **Deploy Changes**.

2. To change network settings on the QRadar Console, use SSH to log in to QRadar as the root user.

   The user name is `root`.

   a. Type the following command: `qchange_netsetup`.

   b. Follow the instructions in the wizard to complete the configuration,

   The following table contains descriptions and notes to help you configure the network settings.

Table 16. Description of network settings for a multisystem QRadar Console deployment

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Optional Used to access the server, usually from a different network or the Internet. Configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. (NAT translates an IP address in one network to a different IP address in another network).
Email server name	If you do not have an email server, use `localhost`.

   After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

3. To readd and reassign the managed hosts, log in to QRadar.

   `https://IP_Address_QRadar`

   The **Username** is `admin`.

   a. Click the **Admin** tab.

   b. Click the **Deployment Editor** icon.

   c. In the Deployment Editor window, click the **System View** tab.

d. Click **Actions** > **Add a managed host**.

e. Follow the instructions in the wizard to add a host.

   Select the **Host is NATed** option to configure a public IP address for the server. This IP address is a secondary IP address that is used to access the server, usually from a different network or the Internet. The Public IP address is often configured by using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network

4. Reassign all components to your managed hosts that are not your QRadar Console.

   a. In the Deployment Editor window, click the **Event View** tab, and select the component that you want to reassign to the managed host.

   b. Click **Actions** > **Assign**.

   c. From the **Select a host list** list, select the host that you want to reassign to this component.

   d. On the **Admin** tab, click **Deploy Changes**.

Updating network settings after a NIC replacement

If you replace your integrated system board or stand-alone (Network Interface Cards) NICs, you must update your IBM Security QRadar network settings to ensure that your hardware remains operational.

About this task

The network settings file contains one pair of lines for each NIC that is installed and one pair of lines for each NIC that was removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

Your network settings file might resemble the following example, where *NAME="eth0* is the NIC that was replaced and *NAME="eth4"* is the NIC that was installed.

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4
```

Procedure

1. Use SSH to log in to the IBM Security QRadar product as the root user.

   The user name is `root`.

2. Type the following command:
   `cd /etc/udev/rules.d/`
3. To edit the network settings file, type the following command:
   `vi 70-persistent-net.rules`
4. Remove the pair of lines for the NIC that was replaced: `NAME="eth0"`.
5. Rename the `Name=<eth>` values for the newly installed NIC.

   Example: Rename `NAME="eth4"` to `NAME="eth0"`.
6. Save and close the file.
7. Type the following command: `reboot`.

Appendix. Troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

Review the following table to help you or customer support resolve a problem.

Table 17. Troubleshooting actions to prevent problems

Action	Description
Apply all known fix packs, service levels, or program temporary fixes (PTF).	A product fix might be available to fix the problem.
Ensure that the configuration is supported.	Review the software and hardware requirements.
Look up error message codes by selecting the product from the IBM Support Portal (http://www.ibm.com/support/entry/portal) and then typing the error message code into the **Search support** box.	Error messages give important information to help you identify the component that is causing the problem.
Reproduce the problem to ensure that it is not just a simple error.	If samples are available with the product, you might try to reproduce the problem by using the sample data.
Check the installation directory structure and file permissions.	The installation location must contain the appropriate file structure and the file permissions. For example, if the product requires write access to log files, ensure that the directory has the correct permission.
Review relevant documentation, such as release notes, technotes, and proven practices documentation.	Search the IBM knowledge bases to determine whether your problem is known, has a workaround, or if it is already resolved and documented.
Review recent changes in your computing environment.	Sometimes installing new software might cause compatibility issues.

If you still need to resolve problems, you must collect diagnostic data. This data is necessary for an IBM technical-support representative to effectively troubleshoot and assist you in resolving the problem. You can also collect diagnostic data and analyze it yourself.

Troubleshooting resources

Troubleshooting resources are sources of information that can help you resolve a problem that you have with a product. Many of the resource links provided can also be viewed in a short video demonstration.

To view the video version, search for "troubleshooting" through either Google search engine or YouTube video community.

Support Portal

The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services.

Use IBM Support Portal to access all the IBM support resources from one place. You can adjust the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Find the IBM Security QRadar content that you need by selecting your products from the IBM Support Portal (http://www.ibm.com/support/entry/portal).

Service requests

Service requests are also known as Problem Management Records (PMRs). Several methods exist to submit diagnostic information to IBM Software Technical Support.

To open a service request, or to exchange information with technical support, view the IBM Software Support Exchanging information with Technical Support page (http://www.ibm.com/software/support/exchangeinfo.html). Service requests can also be submitted directly by using the Service requests (PMRs) tool (http://www.ibm.com/support/entry/portal/Open_service_request) or one of the other supported methods that are detailed on the exchanging information page.

Fix Central

Fix Central provides fixes and updates for your system software, hardware, and operating system.

Use the pull-down menu to go to your product fixes on Fix Central (http://www.ibm.com/support/fixcentral). You might also want to view Getting started with Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html).

Knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods

Use the following knowledge bases to find useful information.

Technotes and APARs

From the IBM Support Portal (http://www.ibm.com/support/entry/portal), you can search technotes and APARs (problem reports).

IBM masthead search

Use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com page.

External search engines

Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com® domain.

However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

QRadar log files

Use the IBM Security QRadar log files to help you troubleshoot problems.

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

1. To help you troubleshoot errors or exceptions, review the following log files.
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. If you require more information, review the following log files:
   - https://*console_ip*/system_info.cgi
   - `/var/log/qradar-sql.log`
   - `/opt/tomcat5/logs/catalina.out`
   - `/opt/imq/share/var/instances/imqbroker/log/log.txt`
   - `/var/log/qflow.debug`
3. To collect log files for an IBM technical-support representative, from the command line, run the following command:

   `/opt/qradar/support/get_logs.sh -s`

   The command creates a `logs_<console_name>_<date_time>.tar.bz2` file in the `/var/log` directory.

Ports used by QRadar

Review the common ports that are used by IBM Security QRadar, services, and components.

For example, you can determine the ports that must be opened for the QRadar Console to communicate with remote Event Processors.

Ports and iptables

The listen ports for QRadar are valid only when iptables is enabled on your QRadar system.

SSH communication on port 22

All the ports that are described in following table can be tunneled, by encryption, through port 22 over SSH. Managed hosts that use encryption can establish multiple bidirectional SSH sessions to communicate securely. These SSH sessions are initiated from the managed host to provide data to the host that needs the data in the deployment. For example, Event Processor appliances can initiate multiple SSH sessions to the QRadar Console for secure communication. This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. QRadar QFlow Collectors that use

encryption can initiate SSH sessions to Flow Processor appliances that require data.

QRadar ports

Unless otherwise noted, information about the assigned port number, descriptions, protocols, and the signaling direction for the port applies to all IBM Security QRadar products.

The following table lists the ports, protocols, communication direction, description, and the reason that the port is used.

Table 18. Listening ports that are used by QRadar, services, and components

Port	Description	Protocol	Direction	Requirement
22	SSH	TCP	Bidirectional from the QRadar Console to all other components.	Remote management access Adding a remote system as a managed host Log source protocols to retrieve files from external devices, for example the log file protocol Users who use the command-line interface to communicate from desktops to the Console High-availability (HA)
25	SMTP	TCP	From all managed hosts to the SMTP gateway	Emails from QRadar to an SMTP gateway Delivery of error and warning email messages to an administrative email contact
37	rdate (time)	UDP/TCP	All systems to the QRadar Console QRadar Console to the NTP or rdate server	Time synchronization between the QRadar Console and managed hosts
80	Apache/HTTPS	TCP	Users that connect to the QRadar Console Users that connect to the QRadar Deployment Editor	Communication and downloads from the QRadar Console to desktops The Deployment Editor application to download and show deployment information
111	Port mapper	TCP/UDP	Managed hosts that communicate to the QRadar Console Users that connect to the QRadar Console	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS)

Table 18. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	WinCollect agents and Windows operating systems that are remotely polled for events. Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter. **Note:** DCOM typically allocates a random port range for communication. You can configure Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.
137	Windows NetBIOS name service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
138	Windows NetBIOS datagram service	UDP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter..

Table 18. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
139	Windows NetBIOS session service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.
199	NetSNMP	TCP	QRadar managed hosts that connect to the QRadar Console External log sources to QRadar Event Collectors	TCP port for the NetSNMP daemon that listens for communications (v1, v2c, and v3) from external log sources
443	Apache/HTTPS	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console	Configuration downloads to managed hosts from the QRadar Console QRadar managed hosts that connect to the QRadar Console Users to have log in access to QRadar QRadar Console that manage and provide configuration updates WinCollect agents
445	Microsoft Directory Service	TCP	Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events Bidirectional traffic between QRadar Console components or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by WinCollect, Microsoft Security Event Log Protocol, or Adaptive Log Exporter.

Table 18. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
514	Syslog	UDP/TCP	External network appliances that provide TCP syslog events use bidirectional traffic. External network appliances that provide UDP syslog events use uni-directional traffic.	External log sources to send event data to QRadar components Syslog traffic includes WinCollect agents and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar
762	Network File System (NFS) mount daemon (mountd)	TCP/UDP	Connections between the QRadar Console and NFS server	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging	Internal logging port for syslog-ng
2049	NFS	TCP	Connections between the QRadar Console and NFS server	The Network File System (NFS) protocol to share files or data between components
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QRadar QFlow Collector.	NetFlow datagram from components, such as routers
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar offense resolution
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance	Required for provisioning managed hosts from the **Admin** tab
6543	High-availability heartbeat	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host Ports 7676 and 7677 are static TCP ports and four extra connections are created on random ports.

Table 18. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
7777 - 7782, 7790, 7791	JMX server ports	TCP	Internal communications, these ports are not available externally	JMX server (Mbean) monitoring for ECS, hostcontext, Tomcat, VIS, reporting, ariel, and accumulator services **Note:** These ports are used by QRadar support.
⌂7789	HA Distributed Replicated Block Device	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Distributed Replicated Block Device is used to keep drives synchronized between the primary and secondary hosts in HA configurations
7800	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for events
7801	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for flows
7803	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Anomaly detection engine port
8000	Event Collection service (ECS)	TCP	From the Event Collector to the QRadar Console	Listening port for specific Event Collection service (ECS).
8001	SNMP daemon port	UDP	External SNMP systems that request SNMP trap information from the QRadar Console	UDP listening port for external SNMP data requests.
8005	Apache Tomcat	TCP	None	A local port that is not used by QRadar
8009	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service
8080	Apache Tomcat	TCP	From the HTTP daemon (HTTPd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector	NetFlow datagram from components, such as routers
10000	QRadar web-based, system administration interface	TCP/UDP	User desktop systems to all QRadar hosts	Server changes, such as the hosts root password and firewall access
23111	SOAP web server	TCP		SOAP web server port for the event collection service (ECS)
23333	Emulex Fibre Channel	TCP	User desktop systems that connect toQRadar appliances with a Fibre Channel card	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt)

Table 18. Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Requirement
32004	Normalized event forwarding	TCP	Bidirectional between QRadar components	Normalized event data that is communicated from an off-site source or between Event Collectors
⌂32005	Data flow	TCP	Bidirectional between QRadar components	Data flow communication port between Event Collectors when on separate managed hosts
32006	Ariel queries	TCP	Bidirectional between QRadar components	Communication port between the Ariel proxy server and the Ariel query server
32009	Identity data	TCP	Bidirectional between QRadar components	Identity data that is communicated between the passive vulnerability information service (VIS) and the Event Collection service (ECS)
32010	Flow listening source port	TCP	Bidirectional between QRadar components	Flow listening port to collect data from QRadar QFlow Collectors
32011	Ariel listening port	TCP	Bidirectional between QRadar components	Ariel listening port for database searches, progress information, and other associated commands
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components	Data flows, such as events, flows, flow context, and event search queries
40799	PCAP data	TCP	From Juniper Networks SRX Series appliances to QRadar	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances. **Note:** The packet capture on your device can use a different port. For more information about configuring packet capture, see your Juniper Networks SRX Series appliance documentation
ICMP	ICMP		Bidirectional traffic between the secondary host and primary host in an HA cluster	Testing the network connection between the secondary host and primary host in an HA cluster by using Internet Control Message Protocol (ICMP)

Searching for ports in use by QRadar

Use the **netstat** command to determine which ports are in use on the QRadar Console or managed host. Use the **netstat** command to view all listening and established ports on the system.

Procedure

1. Using SSH, log in to your QRadar Console, as the root user.
2. To display all active connections and the TCP and UDP ports on which the computer is listening, type the following command:

   ```
   netstat -nap
   ```

3. To search for specific information from the netstat port list, type the following command:

   ```
   netstat -nap | grep port
   ```

   Examples:

   - To display all ports that match 199, type the following command: `netstat -nap | grep 199`
   - To display all postgres related ports, type the following command: `netstat -nap | grep postgres`
   - To display information on all listening ports, type the following command: `netstat -nap | grep LISTEN`

Viewing IMQ port associations

You can view port numbers associations for messaging connections (IMQ) application services are allocated. To look up the additional port numbers, connect to the localhost by using telnet.

Important: Random port associations are not static port numbers. If a service is restarted, the ports that generated for a service are reallocated and the service is assigned a new set of port numbers.

Procedure

1. Using SSH to log in to the QRadar Console, as the root user.
2. To display a list of associated ports for the IMQ messaging connection, type the following command:

   ```
   telnet localhost 7676
   ```

3. If no information is displayed, press the Enter key to close the connection.

Notices

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

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

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

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

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

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

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

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

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

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

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

The following terms are trademarks or registered trademarks of other companies:

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and

IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

Printed in USA