IBM Security QRadar
Version 7.2.6

Installation Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 55.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to QRadar installations

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

Thank you for ordering your appliance from IBM! It is strongly recommended that you apply the latest maintenance to you appliance for the best results. Please visit IBM Fix Central (http://www.ibm.com/support/fixcentral) to determine the latest recommended patch for your product.

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

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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 lawful 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.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. QRadar deployment overview

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

For maximum performance and scalability, you must install a high-availability (HA) managed host appliance 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 appliances, 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 pre-installed with QRadar software, the activation key is included in a document 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 temporary 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 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
User limit	10
Network object limit	300

When you purchase a QRadar product, an email that contains your permanent license key 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.

Related tasks:

Chapter 3, "Installing a QRadar Console or managed host," on page 15
Install IBM Security QRadar Console or a managed host on the QRadar appliance or on your own appliance.

"Installing RHEL on your own appliance" on page 20
You can install the Red Hat Enterprise Linux operating system on your own appliance for use with IBM Security QRadar.

"Installing the QRadar software on a virtual machine" on page 28
After you create your virtual machine, you must install the IBM Security QRadar software on the virtual machine.

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 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 Integrated Management Module, see the *Integrated Management Module User's Guide* on the CD that is shipped with your appliance.

Related concepts:

"Prerequisite hardware accessories and desktop software for QRadar installations" on page 5
Before you install IBM Security QRadar products, ensure that you have access to the required hardware accessories and desktop software.

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 are not supported.

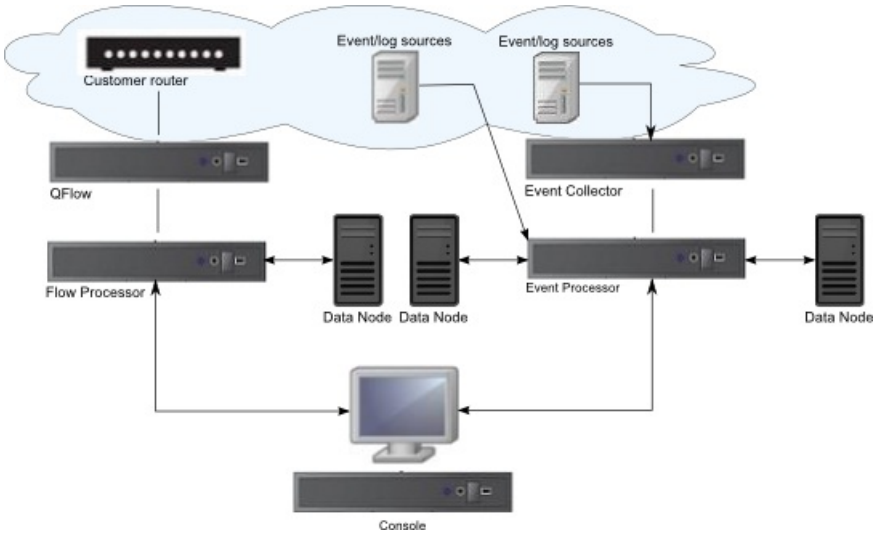

Figure 1. QRadar deployment example

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 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.

Magistrate
A service running on the QRadar Console, the 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.

QRadar Event Collector

Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component, on the QRadar Console, 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

- Use the QRadar Event Collector 1501 in remote locations with slow WAN links. The Event Collector appliances do not store events locally. Instead, the appliances collect and parse events before sending events to an Event Processor appliance for storage.
- The Event Collector can use bandwidth limiters and schedules to send events to the Event Processor to avoid WAN limitations.
- The Event Collector is assigned to an EPS license that matches the Event Processor that it is connected to.

.

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.

When to add Event Processors

- If your event rate exceeds the rating for an QRadar 3105 (All-in-One), 5000 EPS, you must add a QRadar Event Processor 1605 or a QRadar Event Processor 1628.
- If you collect and store events in a different country or state, you may need to add Event Processors to comply with local data collection laws.

Data Node

Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Notes increase the search speed on your deployment by allowing you to keep more of your data uncompressed.

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

QRadar appliance sizing

The following table provides guidance for when to use specific QRadar appliances in your deployment.

Table 3. QRadar appliance overview

Appliance	Description
QRadar 2100	A non-expandable solution for deployments with 10-200 employees.
QRadar 3105 (All-in-One)	Offers increased capacity over the QRadar 2100, and offers the ability to add Event Processors and Flow Processors.

Table 3. QRadar appliance overview (continued)

Appliance	Description
QRadar 3105 (Console)	If your deployment processes more than 5000 events per second (EPS), you must use a QRadar 3105 (Console) with distributed Event Processors. The QRadar 3105 (Console) uses offboard event processing and storage to free up resources for serving reports, search results, and faster UI actions.
QRadar 3128 (All-in-One)	Offers increased capacity over the QRadar 3105 (All-in-One).
QRadar 3128 (Console)	Offers increased capacity over the QRadar 3105 (Console).
xx05 collectors and processors	12 processors 64 GB of RAM 6.2 TB of usable storage
xx28 collectors and processors	28 processors 128 GB of RAM 40 TB of usable storage Pair xx28 collectors and processors with the QRadar 3128 (Console) to increase performance.

When to add Flow Processors

- When your netflow collection rate exceeds the flow rating for your 31xx appliance, you must move to a dedicated Flow Processor.
- If you are adding QRadar QFlow Collectors to your deployment, you must add Flow Processors to store and process the QFlow data.
- If you collect and store flows in a different country or state, you may need to add Flow Processors to comply with local data collection laws.

Related concepts:

Chapter 11, "Troubleshooting problems," on page 51
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.

Chapter 9, "Data Node Overview," on page 43
Understand how to use Data Nodes in your IBM Security QRadar deployment.

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.

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 do not support software-based RAID installations.

Desktop software requirements

Ensure that Java™ Runtime Environment (JRE) version 1.7 or IBM 64-bit Runtime Environment for Java V7.0 is installed on all desktop systems that you use to access the QRadar product user interface.

Related tasks:

Chapter 3, "Installing a QRadar Console or managed host," on page 15
Install IBM Security QRadar Console or a managed host on the QRadar appliance or on your own appliance.

"Installing RHEL on your own appliance" on page 20
You can install the Red Hat Enterprise Linux operating system on your own appliance for use with IBM Security QRadar.

"Installing the QRadar software on a virtual machine" on page 28
After you create your virtual machine, you must install the IBM Security QRadar software on the virtual machine.

Firmware update

Update the firmware on IBM Security QRadar appliances to take advantage of additional features and updates for the internal hardware components of the QRadar appliance.

For more information about updating firmware, see Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121).

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 4. Supported web browsers for QRadar products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
32-bit or 64-bit Microsoft Internet Explorer, with document mode or browser mode enabled.	10.0

Table 4. Supported web browsers for QRadar products (continued)

Web browser	Supported versions
64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.	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.

Related concepts:

"Prerequisite hardware accessories and desktop software for QRadar installations" on page 5
Before you install IBM Security QRadar products, ensure that you have access to the required hardware accessories and desktop software.

USB flash drive installations

You can install IBM Security QRadar software with a USB flash drive.

USB flash drive installations are full product installations. You cannot use a USB flash drive to upgrade or apply product patches. For information about applying fix packs, see the fix pack Release Notes.

Supported versions

The following appliances or operating systems can be used to create a bootable USB flash drive:

- A QRadar v7.2.1 appliance or later
- A Linux system that is installed with Red Hat Enterprise Linux 6.7
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

Installation overview

Follow this procedure to install QRadar software from a USB flash drive:

1. Create the bootable USB flash drive.
2. Install the software for your QRadar appliance.
3. Install any product maintenance releases or fix packs.

See the Release Notes for installation instructions for fix packs and maintenance releases.

Creating a bootable USB flash drive with a QRadar appliance

You can use an IBM Security QRadar V7.2.1 or later appliance to create a bootable USB flash drive that can be used to install QRadar software.

Before you begin

Before you can create a bootable USB flash drive from a QRadar appliance, you must have access to the following items:

- A 2 GB USB flash drive
- A QRadar V7.2.1 or later ISO image file
- A physical QRadar appliance

If your QRadar appliance does not have Internet connectivity, you can download the QRadar ISO image file to a desktop computer or another QRadar appliance with Internet access. You can then copy the ISO file to the QRadar appliance where you install the software.

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

Procedure

1. Download the QRadar ISO image file.
   a. Access the IBM Support website (www.ibm.com/support).
   b. Locate the IBM Security QRadar ISO file that matches the version of the QRadar appliance.
   c. Copy the ISO image file to a `/tmp` directory on your QRadar appliance.
2. Using SSH, log in to your QRadar system as the root user.
3. Insert the USB flash drive in the USB port on your QRadar system.
   It might take up to 30 seconds for the system to recognize the USB flash drive.
4. Type the following command to mount the ISO image:
   `mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom`
5. Type the following commend to copy the USB creation script from the mounted ISO to the `/tmp` directory.
   `cp /media/cdrom/post/create-usb-key.py /tmp/`
6. Type the following command to start the USB creation script:
   `/tmp/create-usb-key.py`
7. Press `Enter`.
8. Press `1` and type the path to the ISO file. For example,
   `/tmp/<name of the iso image>.iso`
9. Press `2` and select the drive that contains your USB flash drive.
10. Press `3` to create your USB key.
    The process of writing the ISO image to your USB flash drive takes several minutes to complete. When the ISO is loaded onto the USB flash drive, a confirmation message is displayed.
11. Press `q` to quit the USB key script.
12. Remove the USB flash drive from your QRadar system.
13. To free up space, remove the ISO image file from the `/tmp` file system.

What to do next

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing QRadar with a USB flash drive.

Creating a bootable USB flash drive with Microsoft Windows

You can use a Microsoft Windows desktop or notebook system to create a bootable USB flash drive that can be used to install QRadar software.

Before you begin

Before you can create a bootable USB flash drive with a Microsoft Windows system, you must have access to the following items:

- A 2 GB USB flash drive
- A desktop or notebook system with one the following operating systems:
  - Windows 7
  - Windows Vista
  - Windows 2008
  - Windows 2008R2

You must download the following files from the IBM Support website (www.ibm.com/support).

- QRadar V7.2.1 or later, Red Hat 64-bit ISO image file
- Create-USB-Install-Key (CUIK) tool.

You must download the following files from the Internet.

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

Tip: Search the web for `Peazip Portal v4.8.1` and `Syslinux` to find the download files.

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

Procedure

1. Extract the Create-USB-Install-Key (CUIK) tool to the `c:\cuik` directory.
2. Copy the `.zip` files for PeaZip Portable 4.8.1 and SYSLINUX 4.06 to the `cuik\deps` folder.

   For example, `c:\cuik\deps\peazip_portable-4.8.1.WINDOWS.zip` and `c:\cuik\deps\syslinux-4.06.zip`.

   You do not need to extract the `.zip` files. The files need only to be available in the `cuik/deps` directory.
3. Insert the USB flash drive into the USB port on your computer.
4. Verify that the USB flash drive is listed by drive letter and that it is accessible in Microsoft Windows.
5. Right-click on `c:\cuik\cuik.exe`, select **Run as administrator**, and press **Enter**.
6. Press 1, select the QRadar ISO file, and click **Open**.

7. Press 2 and select the number that corresponds to the drive letter assigned to your USB flash drive.
8. Press 3 to create the USB flash drive.
9. Press **Enter** to confirm that you are aware that the contents of the USB flash drive will be deleted.
10. Type `create` to create a bootable USB flash drive from the ISO image. This process takes several minutes.
11. Press **Enter**, and then type `q` to exit the Create_USB_Install_Key tool.
12. Safely eject the USB flash drive from your computer.

What to do next

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing QRadar with a USB flash drive.

Creating a bootable USB flash drive with Red Hat Linux

You can use a Linux desktop or notebook system with Red Hat v6.7 to create a bootable USB flash drive that can be used to install IBM Security QRadar software.

Before you begin

Before you can create a bootable USB flash drive with a Linux system, you must have access to the following items:

- A 2 GB USB flash drive
- A QRadar V7.2.1 or later ISO image file
- A Linux system that has the following software installed:
  - Red Hat 6.7
  - Python 6.2 or later

When you create a bootable USB flash drive, the contents of the flash drive are deleted.

Procedure

1. Download the QRadar ISO image file.
   a. Access the IBM Support website (www.ibm.com/support).
   b. Locate the IBM Security QRadar ISO file.
   c. Copy the ISO image file to a `/tmp` directory on your QRadar appliance.
2. Update your Linux- based system to include these packages.
   - syslinux
   - mtools
   - dosfstools
   - parted

   For information about the specific package manager for your Linux system, see the vendor documentation.
3. Log in to your QRadar system as the root user.
4. Insert the USB flash drive in the front USB port on your system.

   It might take up to 30 seconds for the system to recognize the USB flash drive.

5. Type the following command to mount the ISO image:
   `mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom`
6. Type the following command to copy the USB creation script from the mounted ISO to the `/tmp` directory.
   `cp /media/cdrom/post/create-usb-key.py /tmp/`
7. Type the following command to start the USB creation script:
   `/tmp/create-usb-key.py`
8. Press `Enter`.
9. Press `1` and type the path to the ISO file. For example,
   `/tmp/Rhe664QRadar7_2_4_<build>.iso`
10. Press `2` and select the drive that contains your USB flash drive.
11. Press `3` to create your USB key.
    The process of writing the ISO image to your USB flash drive takes several minutes to complete. When the ISO is loaded onto the USB flash drive, a confirmation message is displayed.
12. Press `q` to quit the USB key script.
13. Remove the USB flash drive from your system.

What to do next

If your connection to the appliance is a serial connection, see Configuring a flash drive for serial only appliances.

If your connection to the appliance is keyboard and mouse (VGA), see Installing QRadar with a USB flash drive.

Configuring a USB flash drive for serial-only appliances

You must complete an extra configuration step before you can use the bootable USB flash drive to install QRadar software on serial-only appliances.

About this task

This procedure is not required if you have a keyboard and mouse that is connected to your appliance.

Procedure

1. Insert the bootable USB flash drive into the USB port of your appliance.
2. On your USB flash drive, locate the `syslinux.cfg` file.
3. Edit the syslinux configuration file to change the default installation from `default linux` to `default serial`.
4. Save the changes to the syslinux configuration file.

What to do next

You are now ready to install QRadar with the USB flash drive.

Installing QRadar with a USB flash drive

Follow this procedure to install QRadar from a bootable USB flash drive.

Before you begin

You must create the bootable USB flash drive before you can use it to install QRadar software.

About this task

This procedure provides general guidance on how to use a bootable USB flash drive to install QRadar software.

The complete installation process is documented in the product Installation Guide.

Procedure

1. Install all necessary hardware.
2. Choose one of the following options:
   - Connect a notebook to the serial port at the back of the appliance.
   - Connect a keyboard and monitor to their respective ports.
3. Insert the bootable USB flash drive into the USB port of your appliance.
4. Restart the appliance.

   Most appliances can boot from a USB flash drive by default. If you are installing QRadar software on your own hardware, you might have to set the device boot order to prioritize USB.

   After the appliance starts, the USB flash drive prepares the appliance for installation. This process can take up to an hour to complete.
5. When the **Red Hat Enterprise Linux** menu is displayed, select one of the following options:
   - If you connected a keyboard and monitor, select **Install or upgrade using VGA console**.
   - If you connected a notebook with a serial connection, select **Install or upgrade using Serial console**.
6. Type `SETUP` to begin the installation.
7. When the login prompt is displayed, type `root` to log in to the system as the root user.

   The user name is case-sensitive.
8. Press **Enter** and follow the prompts to install QRadar.

   The complete installation process is documented in the product Installation Guide.

Third-party software on QRadar appliances

IBM Security QRadar is a security appliance that is built on Linux, and is designed to resist attacks. QRadar is not intended as a multi-user, general-purpose server. It is designed and developed specifically to support its intended functions. The operating system and the services are designed for secure operation. QRadar has a built-in firewall, and allows administrative access only through a secure connection that requires encrypted and authenticated access, and provides controlled upgrades and updates. QRadar does not require or support traditional anti-virus or malware agents, or support the installation of third-party packages or programs.

Chapter 2. Bandwidth for managed hosts

Plan for the managed hosts bandwidth usage in your IBM Security QRadar deployment.

To replicate state and configuration data, ensure that you have a minimum bandwidth of 100 Mbps between the QRadar console and all managed hosts.

Higher bandwidth is necessary when you search log and network activity, and you have over 10,000 events per second (EPS). System and network performance affect your data search speed. QRadar Event Collectors, with the store and forward configuration, forward all data based on your schedule. You must allocate sufficient bandwidth for the data that you plan to collect, or your store and forward appliance cannot maintain your scheduled pace.

You can mitigate bandwidth limitations between data centers, by using the following methods:

Process and send data to hosts at the primary data center
Design your deployment to process and send data to hosts at the primary data center, where the console resides, as the data is collected. In this design, all user-based searches query the data from the local data center, rather than waiting for remote sites to send back data. You can deploy a store and forward event collector, such as a QRadar 15XX physical or virtual appliance, in the remote locations to control bursts of data across the network. Bandwidth is used in the remote locations, and searches for data occur at the primary data center, rather than at a remote location.

Don't run long-term searches over limited bandwidth connections
Ensure that users don't run long-term searches over links that have limited bandwidth. Searches that have precise filters limit the amount of data that is retrieved from the remote locations and reduces the amount of bandwidth that is required to send data back for the result.

For more information about deploying managed hosts and components after installation, see the *IBM Security QRadar SIEM Administration Guide*.

Chapter 3. 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.

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.
- A keyboard and monitor are connected by using the VGA connection.
- The activation key is available.
- If you want to configure bonded network interfaces, see www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).

Procedure

1. Type `setup` to proceed and log in as root.
2. Accept the Internal Program License Agreement.

   Tip: Press the Spacebar key to advance through the document.
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**, Enterprise model, and set up the time.
5. Select the Internet Protocol version:
   - Select **Yes** to auto-configure QRadar for IPv6.
   - Select **No** to configure an IP address manually QRadar for IPv4 or IPv6.
6. Select the bonded interface set up if required.
7. Select the management interface.
8. In the wizard, enter a fully qualified domain name in the **Hostname** field.
9. In the **IP address** field, enter a static IP address, or use the assigned IP address.

   Important: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

   For more information, see the *IBM Security QRadar High Availability Guide*.
10. If you do not have an email server, enter `localhost` in the **Email server name** field.
11. In the **Root password** field, create a password that meets the following criteria:
    - Contains at least 5 characters

- Contains no spaces
- Can include the following special characters: @, #, ^, and *.

12. Click **Finish**.
13. Follow the instructions in the installation wizard to complete the installation.
    The installation process might take several minutes.
14. Apply your license key.
    a. Log in to QRadar:
       `https://IP_Address_QRadar`
       The default user name is `admin`. The password is the password of the root user account.
    b. Click **Login To QRadar**.
    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 your license key.
    g. Select the unallocated license and click **Allocate System to License**.
    h. From the list of systems, select a system, and click **Allocate System to License**.
15. If you want to add managed hosts, see the *IBM Security QRadar SIEM Administration Guide*.

What to do next

Go to the (https://apps.xforce.ibmcloud.com/) to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *IBM Security QRadar SIEM Administration Guide*.

Chapter 4. QRadar software 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.

Important: Install no software other than QRadar and Red Hat Enterprise Linux on your appliance.

If you are installing QRadar software on your own hardware, you can now purchase the RHEL license as part of the QRadar software purchase, and use the RHEL that ships with the QRadar software ISO image.

Install RHEL separately if your QRadar purchase does not include the RHEL operating system. If your QRadar system does include RHEL, you do not need to configure partitions and perform other RHEL preparation. Proceed to Chapter 3, "Installing a QRadar Console or managed host," on page 15.

Important: Do not install RPM packages that are not approved by IBM. Unapproved RPM installations can cause dependency errors when you upgrade QRadar software and can also cause performance issues in your deployment. Do not use YUM to update your operating system or install unapproved software on QRadar systems.

Prerequisites for installing QRadar 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 5. System requirements for RHEL installations on your own appliance

Requirement	Description
Supported software version	Version 6.7
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 32 GB **Important:** You must upgrade your system memory before you install QRadar.
Memory (RAM) for Event Processor	24 GB
Memory (RAM) for QRadar QFlow Collector	16 GB

Table 5. System requirements for RHEL installations on your own appliance (continued)

Requirement	Description
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.

Note: EFI installations are not supported.

Preparing QRadar software installations for HA and XFS file systems

As part of configuring high availability (HA), the QRadar installer requires a minimal amount of free space in the storage file system, `/store/`, for replication processes. Space must be allocated in advance because XFS file systems cannot be reduced in size after they are formatted.

To prepare the XFS partition for use with HA systems, you must do the following tasks:

1. Use the **`mkdir`** command to create the following directories:
   - `/media/cdrom`
   - `/media/redhat`
2. Mount the QRadar software ISO image by typing the following command:
   `mount -o loop <path_to_QRadar_iso> /media/cdrom`
3. Mount the RedHat Enterprise Linux V6.7 software by typing the following command:
   `mount -o loop <path_to_RedHat_6.7_64bit_dvd_iso_1> /media/redhat`
4. If your system is designated as the primary host in an HA pair, run the following script:
   `/media/cdrom/post/prepare_ha.sh`
5. To begin the installation, type the following command:
   `/media/cdrom/setup`

Note: This procedure is not required on your HA secondary host.

Linux operating system partition properties for QRadar installations on 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 re-create the partitioning on your Red Hat Enterprise Linux operating system.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Table 6. 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	No	SDA
/store/tmp	Storage area for QRadar temporary files	/store/tmp	EXT4	20000 MB	No	SDA
/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	[1]On Console appliances: approximately 80% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: approximately 90% of the available storage.	No	SDA If 2 disks, SDB

Table 6. Partition guide for RHEL (continued)

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/store/transient	Storage area for ariel database cursor	/store/transient	XFS on Consoles EXT4 on managed hosts	[1]On Console appliances: 20% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: 10% of the available storage.	No	SDA If 2 disks, SDB
[1]The /store and /store/transient together take 100% of the disk space that remains after you create the first 5 partitions.						

Restrictions

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

- /store
- /store/tmp
- /store/ariel
- /store/transient

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.

About this task

Install RHEL separately if your QRadar installation does not include the RHEL operating system. If your QRadar system does include RHEL, proceed to Chapter 4, "QRadar software installations on your own appliance," on page 17.

Procedure

1. Copy the Red Hat Enterprise Linux 6.7 operating system DVD ISO to one of the following portable storage devices:
   - Digital Versatile Disk (DVD)
   - Bootable USB flash drive
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`, `store/tmp`, and `/var/log` partitions.

      For more information about file system types based on appliance types, see "Linux operating system partition properties for QRadar installations on your own appliance" on page 18.
   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 operating system partition properties for QRadar installations on your own appliance" on page 18
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 5. 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.

Restriction: Resizing logical volumes by using a logical volume manager (LVM), and EFI installations are not supported.

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.

Important: Install no software other than QRadar and Red Hat Enterprise Linux on the virtual machine.

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 function 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 3199

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 3199 virtual appliance includes an on-board Event Collector and internal storage for events.

The QRadar SIEM All-in-One Virtual 3199 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 (more 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 3199 beyond the license-based upgrade options, you can add one or more of the QRadar SIEM Event Processor Virtual 1699 or QRadar SIEM Flow Processor Virtual 1799 virtual appliances:

QRadar SIEM Flow Processor Virtual 1799

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 1799 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 1799 appliances to any QRadar SIEM 3105 or QRadar SIEM 3124 series appliance to increase the storage and performance of your deployment.

QRadar SIEM Event Processor Virtual 1699

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 1699 includes an on-board Event Collector, Event Processor, and internal storage for events.

The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:

- Up to 20,000 events per second
- 2 TB or larger dedicated event storage

The QRadar SIEM Event Processor Virtual 1699 virtual appliance is a distributed Event Processor appliance and requires a connection to any QRadar SIEM 3105 or QRadar SIEM 3124 series appliance.

QRadar Data Node Virtual 1400

This virtual appliance provides retention and storage for events and flows. The virtual appliance expands the available data storage of Event Processors and Flow Processors, and also improves search performance.

Size your QRadar Data Node Virtual 1400 appliance appropriately, based on the EPS rate and data retention rules of the deployment.

Data retention policies are applied to a QRadar Data Node Virtual 1400 appliance in the same way that they are applied to stand-alone Event Processors and Flow Processors. The data retention policies are evaluated on a node-by-node basis. Criteria, such as free space, is based on the individual QRadar Data Node Virtual 1400 appliance and not the cluster as a whole.

Data Nodes can be added to the following appliances:

- Event Processor (16XX)

- Flow Processor (17XX)
- Event/Flow Processor (18XX)
- All-In-One (2100 and 31XX)

To enable all features included in the QRadar Data Node Virtual 1400 appliance, install using the 1400 activation key.

QRadar VFlow Collector 1299

This virtual appliance provides the same visibility and function 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 1299 virtual appliance supports a maximum of the following items:

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

The QRadar VFlow Collector 1299 virtual appliance does not support NetFlow.

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 7. Requirements for virtual appliances

Requirement	Description
VMware client	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 For more information about VMWare clients, see the VMware website (www.vmware.com)
Virtual disk size on QRadar VFlow Collector, QRadar Event Collector, QRadar Event Processor, QRadar Flow Processor, QRadar All-in-One, and QRadar Log Manager 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
Virtual disk size for QRadar Risk Manager appliances	Suggested virtual disk size for implementation with up to 10000 configuration sources: 1 TB.

Table 7. Requirements for virtual appliances (continued)

Requirement	Description
Virtual disk size for QRadar Vulnerability Manager processor appliances	50000 IP addresses - 500 GB 150000 IP addresses - 750 GB 300000 IP addresses - 1 TB
Virtual disk size for QRadar Vulnerability Manager scanner appliances	20000 IP addresses - 150 GB

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

Table 8. Minimum and optional memory requirements for QRadar virtual appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar VFlow Collector 1299	6 GB	6 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 8090	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
QRadar Vulnerability Manager Processor	8 GB	16 GB
QRadar Vulnerability Manager Scanner	2 GB	4 GB

*Table 9. Sample **CPU** page settings*

Number of processors	Performance based on QRadar appliances
4	Log manager 3190: 2500 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 2500 events per second or less. All-in-One 3190: 25000 flows per minute or less, 500 events per second or less. Flow Processor 1790: 150,000 flows per minute. Dedicated Console 3190

Table 9. Sample **CPU** *page settings (continued)*

Number of processors	Performance based on QRadar appliances
8	Log manager 3190: 5000 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 5000 events per second or less. All-in-One 3190: 50000 flows per minute or less, 1000 events per second or less. Flow Processor 1790: 300,000 flows per minute.
12	All-in-One 3190: 100,000 flows per minute or less, 1000 events per second or less.
16	Log manager Event Processor 1690, or SIEM Event Processor 1690: 20,000 events per second or less. All-in-One 3190: 200,000 flows per minute or less, 5000 events per second or less.

Related tasks:

"Creating your virtual machine"
To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

Creating your virtual machine

To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

Procedure

1. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
2. Add the **Name and Location**, and select the **Datastore** for the new virtual machine.
3. 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 **Linux**, and 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. For more information about CPU settings, see "System requirements for virtual appliances" on page 25.
   e. In the **Memory Size** field, type or select the RAM required for your deployment. For more information about memory requirements, see "System requirements for virtual appliances" on page 25.
   f. Use the following table to configure you network connections.

Table 10. 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 11. Settings for the virtual disk size and provisioning policy parameters

Property	Option
Capacity	256 or higher (GB)
Disk Provisioning	Thin provision
Advanced options	Do not configure

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

What to do next

Install the QRadar software on your virtual machine.

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 Type** pane, select **DataStore ISO File**.
6. In the **Device Status** pane, select the **Connect at power on** check box.
7. In the **Device Type** pane, click **Browse**.
8. In the Browse Datastores window, locate and select the QRadar product ISO file, click **Open** and then click **OK**.
9. After the QRadar product ISO image is installed, right-click your virtual machine and click **Power** > **Power On.**
10. Log in to the virtual machine by typing `root` for the user name.

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

    Tip: Press the Spacebar key to advance through the document.
12. 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.
13. For the type of setup, select **normal**, Enterprise model, and set up the time.

14. Select the Internet Protocol version:
    - Select **Yes** to auto-configure QRadar for IPv6.
    - Select **No** to configure an IP address manually QRadar for IPv4 or IPv6.
15. Select the bonded interface set up if required.
16. Select the management interface.
17. In the wizard, enter a fully qualified domain name in the **Hostname** field.
18. In the **IP address** field, enter a static IP address, or use the assigned IP address.

    Important: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

    For more information, see the *IBM Security QRadar High Availability Guide*.
19. If you do not have an email server, enter `localhost` in the **Email server name** field.
20. In the **Root password** field, create a password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
21. Click **Finish**.
22. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.
23. Apply your license key.
    a. Log in to QRadar:

       `https://`*`IP_Address_QRadar`*

       The default user name is `admin`. The password is the password of the root user account.
    b. Click **Login To QRadar**.
    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 your license key.
    g. Select the unallocated license and click **Allocate System to License**.
    h. From the list of systems, select a system, and click **Allocate System to License**.

What to do next

Go to the (https://apps.xforce.ibmcloud.com/) to download *Security applications* for your installation. For more information, see the *Content Management* chapter in the *IBM Security QRadar SIEM Administration Guide*.

Related tasks:

"Creating your virtual machine" on page 27
To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

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 user name is `admin`. The password is the password of the root user account.
   b. Click **Login To QRadar**.
   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 your license key.
   g. Select the unallocated license and click **Allocate System to License**.
   h. From the list of systems, select a system, and click **Allocate System to License**.

Related tasks:

"Creating your virtual machine" on page 27
To install a virtual appliance, you must first use VMWare ESX to create a virtual machine.

Chapter 6. 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.

The warning message states that you can retain the data on the appliance. This data includes events and flows. Selecting the retain option backs up the data before the reinstallation, and restores the data after installation completes. If the retain option is not available, the partition where the data resides may not be available, and it is not possible to back up and restore the data. The absence of the retain option can indicate a hard disk failure. Contact Customer Support if the retain option is not available.

Important: The retain option is not available on High-Availability systems. See the *IBM Security QRadar High Availability Guide* for information on recovering High-Availability appliances.

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.

Reinstalling 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 offboard storage, see the *Offboard Storage Guide*.

Procedure

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

   The installer partitions and reformats the hard disk, installs the OS, and then re-installs the QRadar product. You must wait for the flatten or retain 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.
8. Apply your license key.
   a. Log in to QRadar:

      `https://IP_Address_QRadar`

      The default user name is `admin`. The password is the password of the root user account.
   b. Click **Login To QRadar**.
   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 your license key.
   g. Select the unallocated license and click **Allocate System to License**.
   h. From the list of systems, select a system, and click **Allocate System to License**.

Chapter 7. Setting up silent installations for QRadar

Install IBM Security QRadar "silently," or perform an unattended installation.

Before you begin

This installation requires the Red Hat Enterprise Linux operating system, and the QRadar V7.2.6 ISO. For information about version numbers and requirements, see Chapter 4, “QRadar software installations on your own appliance,” on page 17.

Procedure

1. Install RHEL on the host where you want to install QRadar to set up the necessary partitions. For more information, see “Installing RHEL on your own appliance” on page 20.
2. As the root user, use SSH to log on to the host where you want to install QRadar.
3. On the host where you want to install QRadar, go to the root directory and create a file that is named `AUTO_INSTALL_INSTRUCTIONS` and that contains the following information:

   Example: The following AUTO_INSTALL_INSTRUCTIONS file example shows the correct parameters for silently installing QRadar in the America/Moncton timezone.

   ```
   timezone=America/Moncton
   sectempl=Enterprise
   date=2015/05/19
   ntpserver=q1dc04.canlab.ibm.com
   ntpsync=1
   timechoice=manual
   nicid=eth0
   box_ip=1.2.3.4
   ip_v6=
   netmask=255.255.255.255
   ipverchoice=ipv4
   gateway_v6=
   hostname=name
   pdns=1.2.3.4
   bdns=5.6.7.8
   newkey=######-######-######-######
   defpass=password
   isconsole=yes
   setuptypechoice=normal
   is_ha_appl=0
   isconstandby=yes
   smtpname=localhost
   bonding_interfaces=
   bonding_options=
   bonding_enabled=false
   ```

   Important: The `AUTO_INSTALL_INSTRUCTIONS` file must have no extension.

   Learn more about silent installations:

Table 12. Silent Install File parameters

Parameter	Required?	Description	Permitted values
setuptypechoice	Required	Specifies the type of installation for this host	normal- A standard QRadar managed host or console deployment. recovery - A High Availability (HA) recovery installation on this host.
timezone	Required	The timezone from the TZ database. For more information, see http://timezonedb.com/.	Europe/London America/Montreal America/New_York America/Los_Angeles Asia/Tokyo, and so on.
date	Required	The current date for this host. Use the following format: YYYY/MM/DD format	
timechoice	Required	Specifies how this host obtains the current time	manual - The time that you manually enter in the time parameter. server - Use a Network Time Protocol (NTP) server that is specified by the ntpserver parameter
time	If timechoice is set to manual, then required.	The time for the host in the 24 hour format HH:MM:SS.	
ntpserver	If timechoice is set to server, then required.	The FQHN or IP address of the network time protocol (NTP) server.	
ntpsync	If timechoice is set to server, then required.	Enter 1 to sync with the NTP server, otherwise, enter 0.	
nicid	Required	The identifier for the network interface card	Values: eth0, eth1, eth*x*
management_iface	Required	The identifier for the management interface	Values: eth0, eth1, eth*x*
hostname	Optional	The fully qualified host name for your QRadar system.	
ipverchoice	Required	Specify the IP standard protocol for this host	IPv4, IPv6

Table 12. Silent Install File parameters (continued)

Parameter	Required?	Description	Permitted values
box_ip	If ipverchoice is set to IPv4, then required	The IP address of the host that you are installing the software on	A valid IPv4 address
ip_v6	If ipverchoice is set to IPv6, then required	Enter the IPv6 address of the QRadar installation if required.	A valid IPv6 address
netmask	If ipverchoice is set to IPv4, then required	The netmask for this host	
gateway	If ipverchoice is set to IPv4, then required	The network gateway for this host	A valid IPv4 address
gateway_v6	If ipverchoice is set to IPv6, then required	The network gateway for this host	A valid IPv6 address
ip_v6_nocidr	Optional	The IPv6 address with no Classless Inter-Domain Routing (CIDR).	A valid IPv6 address
pdns	If ipverchoice is set to IPv4, then required	The primary DNS server.	A valid IPv4 address
bdns	If ipverchoice is set to IPv4, then required	The secondary DNS server.	A valid IPv4 address
newkey	Required	The activation key for the QRadar installation.	
defpass	Required	The default root password to use for this host.	
isconsole	Required	Specify whether this host is the console within the deployment	Y - This host is the console in the deployment N - This is not the console and is another type of managed host (Event or Flow Processor, and so on)

Table 12. Silent Install File parameters (continued)

Parameter	Required?	Description	Permitted values
sectempl	If isconsole is set to Y, then required	The security template.	Enterprise - for all SIEM-based hosts Logger - for Log Manager
is_ha_appl	Required	Specifies whether this host is a HA pair or companion host	0 - This host is not an HA appliance/installation 1 - This host is an HA appliance/installation
isconstandby	If isconsole is set to Y, then required.	Specifies whether this host is an HA console standby	0 - This host is not a standby HA console 1 - This host is a standby HA console
clusterip	Optional	Specifies the IP address for the HA cluster.	ip_address
smtpname	Required	Enter the mail server or SMTP name, such as localhost.	
bonding _interfaces	If using bonded interfaces, then required.	The MAC addresses for the interfaces that you are bonding, separated by commas.	mac_addresses
bonding_options	If using bonded interfaces, then required.	The Linux options for bonded interfaces.	**Example:** miimon=100 mode=4 lacp_rate=1
bonding enabled	If using bonded interfaces, then required.	Specifies whether you are using bonded interfaces.	true or false

4. Using an Secure File Transfer Protocol (SFTP) program, such as WinSCP, copy the QRadar ISO to the host where you want to install QRadar.
5. Using a program such as WinSCP, copy the RHEL ISO to the host where you want to install QRadar.
6. Create a /media/cdrom directory by using the following command:
   ```
   mkdir /media/cdrom
   ```
7. Create a /media/redhat directory by using the following command:
   ```
   mkdir /media/redhat
   ```
8. Mount the QRadar ISO by using the following command:
   ```
   mount -o loop <qradar.iso> /media/cdrom
   ```
9. Mount the RHEL ISO by using the following command:
   ```
   mount -o loop <RHEL.iso> /media/redhat
   ```
10. Run the QRadar setup by using the following command:
    ```
    /media/cdrom/setup
    ```

Chapter 8. Overview of QRadar deployment in a cloud environment

You can install instances of IBM Security QRadar software on a cloud server that is hosted by Amazon Web Service. To establish secure communications between on-premises and cloud instances of QRadar, you must configure a VPN connection. You can configure an OpenVPN connection, or use another mechanism, such as a cloud provider VPN infrastructure.

Important: Ensure that the following requirements are met to avoid compromised security data:

- Set a strong root password.
- Allow only specific connections to ports 443 (https), 22 (ssh), 10000 (webmin), and 1194 (UDP, TCP for OpenVPN).

Configure QRadar for the cloud in the following order:

1. Install QRadar on Amazon Web Service (AWS).
2. For cloud and on-premises hosts, define the role:
   - The server endpoint of a VPN tunnel.
   - The client endpoint of a VPN tunnel.
   - The member host that routes traffic that is destined for the VPN tunnel through the local VPN endpoint.
   - None, if a host that has no need to communicate with hosts on the other side of the VPN tunnel.
3. Confirm that the QRadar firewall settings protect your network security.

Configuring a QRadar host on Amazon Web Service

Configure a secure connection between on-premises instances and Amazon Web Services (AWS) instances of IBM Security QRadar.

Before you begin

1. Configure a key pair on AWS.
2. Create an Amazon EC2 instance that meets the following requirements:

Table 13. AWS Instance Requirements

Requirement	Value
Image	`RHEL-6.7_HVM_Beta_20150714-x86_64-1-Hourly-GP2`
Instance type	m4.2xlarge
Storage	3 x 100 GB volumes
Security Group	Your IP addresses from the list, with ports 22 and 443 open.

Important: Commands in this procedure are examples. Values in commands can vary between deployments.

The AWS instance key is required to log in to the instance with SSH.

XFS is not currently supported on the RedHat Enterprise Linux (RHEL) v6.7 loads that are provided by AWS. Use ext4.

Important: High availability (HA) is not supported on AWS QRadar installations.

Procedure

1. Type the following command to log in to the AWS instance by using the key pair that you created when you configured the instance:

   ```
   ssh -i <your_key>.pem ec2-user@<public_IP_address>
   ```

2. Enter the root shell of the AWS instance by using the following command:

   ```
   sudo su -
   ```

3. Determine the device that you want to configure:
   a. Type the `lsblk` command to list device details.
   b. Find the device that has no partitions and has the required storage.

      ```
      [root@ip-172-31-13-123 ~]# lsblk
      NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      xvda
            202:0 0 100G 0 disk
      └─xvda1 202:1 0 100G 0 part /
      xvdc 202:32 0 100G 0 disk
      xvdb 202:16 0 100G 0 disk
      ```

      After you find the block devices, export the device name and device data as environment variables for use in subsequent steps. For the preceding example, you type the following commands:

      ```
      export device_name=/dev/xvdc
      export device_data=/dev/xvdb
      ```

4. To create the partition type for the disk (label), type the following commands:

   ```
   parted -a optimal --script ${device_name} -- mklabel gpt
   parted -a optimal --script ${device_data} -- mklabel gpt
   ```

5. To create these partitions on the device, type the following commands:

   Note: The following allocations are examples. For information about partitions, see the *IBM Security QRadar Installation Guide*.

   ```
   parted -a optimal --script $device_name -- mkpart swap 0% 30%
   parted -a optimal --script ${device_name} -- mkpart ext4 30% 60%
   parted -a optimal --script ${device_name} -- mkpart ext4 60% 100%
   parted -a optimal --script ${device_data} -- mkpart ext4 0% 80%
   parted -a optimal --script ${device_data} -- mkpart ext4 80% 100%
   ```

6. To create the following file systems on the partitioned device, type the following commands:

   ```
   mkswap -L swap1 ${device_name}1
   mkfs.ext4 ${device_name}2
   mkfs.ext4 ${device_name}3
   mkfs.ext4 ${device_data}1
   mkfs.ext4 ${device_data}2
   ```

7. Label the partitions with the following names:

   ```
   e2label ${device_name}2 /var/log
   e2label ${device_name}3 /store/tmp
   e2label ${device_data}2 /store/transient
   e2label ${device_data}1 /store
   ```

8. If the line is present, comment out the `/dev/<device_name> /mnt`, or `/dev/<device_data> /mnt` line in the `/etc/fstab` file.
9. Type the following commands to add the required entries to `/etc/fstab` file:

```
eval `blkid -t LABEL=/store -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab
eval `blkid -t LABEL=/store/transient -o export` ; echo
      UUID=$UUID /store/transient $TYPE defaults,noatime 1 1 >> /etc/fstab
eval `blkid -t LABEL=/var/log -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab
echo  "${device_name}1
 swap  swap defaults 0 0" >> /etc/fstab
```

10. To create and mount the /store directory, type the following commands:

```
mkdir /store
mount /store
mkdir /store/tmp
mount /store/tmp
mkdir /store/transient
mount /store/transient
cd /var; mv log oldlog; mkdir log; mount /var/log; mv oldlog/* log
```

11. To enable the swap between devices, type the following command:

```
swapon -a
```

12. Confirm that the /etc/sysconfig/i18n line contains the following string, including the quotation marks:

```
LANG="en_US.UTF-8"
```

13. To copy the ISO image to the device, type the following command:

```
scp -i key.pem qradar.iso ec2-user@<Public_DNS>:qradar.iso
```

    Where:

    - *qradar.iso* is the name of the QRadar installation ISO image.
    - *key.pem* is the key to log in to the box.
    - *Public_DNS* is the domain name of the host.

14. To mount the ISO image, type the following commands:

```
mkdir /media/cdrom
mount -o loop /home/ec2-user/qradar.iso /media/cdrom
```

15. Configure missing dependencies by using the following commands:

```
yum  install -y libxml2 libxml2.i686 audit-libs audit-libs.i686 glibc
glibc.i686 device-mapper-multipath zlib zlib.i686 libcom_err
libcom_err.i686 nspr nspr.i686 nss nss.i686 nss-util nss-util.i686
krb5-libs krb5-libs.i686 keyutils-libs keyutils-libs.i686
openssl   openssl.i686 httpd-tools httpd-devel httpd mod_ssl keyutils
keyutils.i686 keyutils-libs keyutils-libs.i686 openldap openldap.i686
openldap-clients cyrus-sasl-lib cyrus-sasl-lib.i686 pam pam.i686 libgcc
libgcc.i686 elfutils-libelf  elfutils-libelf.i686
libstdc++   libstdc++.i686
```

```
yum remove php.x86_64 php-cli.x86_64 php-common.x86_64
php-devel.x86_64 php-imap.x86_64 samba-common samba-winbind-clients
samba-client samba-winbind
httpd httpd-tools mod_ssl
```

```
sed -i -e's/plugins=1/plugins=0/' /etc/yum.conf
```

16. To start the setup program, type the following command:

```
/media/cdrom/setup
```

Configuring server endpoints for cloud installations

Use OpenVPN to configure a server endpoint on the cloud server when the IBM Security QRadar console is on-premises, with more processing and storage nodes are installed in the cloud.

About this task

A server endpoint requires the following items:

- A main OpenVPN configuration file.
- Routing instructions for each client in the server configuration file.
- A configuration file for each client that records routing instructions for each client that can connect.
- Additional iptables rules that allow forwarding across the tunnel.
- IP forwarding enabled in the kernel.
- A custom certificate authority (CA) to issue the certificates that are used to authenticate servers and clients.
- A server certificate that is issued by the local CA.

For more information about the OpenVPN tool options, enter `-h`.

Procedure

1. To specify the server endpoint, type the following command to define the server endpoint in the cloud.

   `/opt/qradar/bin/vpntool server` *`server_host_IP_address network_address_behind_VPN`*

   Example:

   `/opt/qradar/bin/vpntool server 1.2.3.4 5.6.7.8/24`

   If your network requires TCP rather than UDP mode on your clients and servers, type the following command with your required IP addresses:

   `/opt/qradar/bin/vpntool server` *`server_host_IP_address network_address_behind_VPN`* `--tcp`

   After you define the server endpoint, VPNtool Server completes the following tasks:

   - If the local certificate authority is not established, the CA is initialized and the CA key and certificate created.
   - The local CA creates a key and certificate for use by this server endpoint.
   - Configuration properties are written to the VPN configuration file.
2. To build and deploy the configuration, type the following command:

   `/opt/qradar/bin/vpntool deploy`

   After you build and deploy the configuration, VPNtool Server completes the following tasks:

   - The OpenVPN server configuration is generated and copied into the `/etc/openvpn` directory.
   - The CA certificate, and the server key and certificate, are copied into the standard location in `/etc/openvpn/pki`.
   - IPtables rules are constructed and reloaded.
   - IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.
3. To start the server, type the following command:

   `/opt/qradar/bin/enable --now`

   Entering `/opt/qradar/bin/enable --now` creates the persistent enabled state, and automatically starts OpenVPN on system restart.

Configuring client networks for cloud installations

In on premises environments, use OpenVPN to configure a client network that communicates with endpoints that are in the cloud.

About this task

A client requires the following items:

- A main OpenVPN configuration file.
- Extra iptables rules to allow forwarding across the tunnel.
- IP forwarding is enabled in the kernel.
- A client certificate that is issued by the local CA.

Procedure

1. On the server, inform the server of the new client, type the following command:

   ```
   /opt/qradar/bin/vpntool addclient Console name, role,
    or IP  1.2.3.4/24
   ```

   Informing the server of the client includes the following tasks:

   - The CA certificate is copied to a known location.
   - The client key and certificate from the PKCS#12 file are extracted and copied to known locations.
   - Client configuration properties are written to the VPN configuration file.

2. Deploy and restart the server by using the following command:

   ```
   /opt/qradar/bin/vpntool deploy
   service openvpn restart
   ```

3. Copy the generated client credentials file and the CA file to the QRadar host that is used for this client endpoint.

   Example:

   ```
   scp root@ server_IP_address :/opt/qradar/conf
   /vpn/pki/ca.crt /root/ca.crtscp root@ server_IP_address
   :/opt/qradar/conf/vpn/pki/Console.p12 /root/Console.p12
   ```

4. On the client, configure the host as a VPN client:

   ```
   /opt/qradar/bin/vpntool client server_IP_address
   ca.crt client.pk12
   ```

   If your network requires that you not configure UDP mode on your clients and servers, you can use TCP.

   ```
   /opt/qradar/bin/vpntool client server_IP_address
   /root/ca.crt /root/Console.p12 --tcp
   ```

5. To build and deploy the configuration, type the following command:

   ```
   /opt/qradar/bin/vpntool deploy
   ```

   Building and deploying the configuration includes the following steps:

   - The client OpenVPN configuration file is generated and copied into place in `/etc/openvpn`.
   - The CA certificate, and client key and certificate, are copied into the standard locations within `/etc/openvpn/pki`.
   - Iptables rules are generated and loaded.
   - IP forwarding is enabled and made persistent by updating the `/etc/sysctl.conf` file.

6. To start the client, enter the following command:

```
/opt/qradar/bin/enable --now
```

Entering `/opt/qradar/bin/enable --now` creates the persistent enabled state, and automatically starts OpenVPN on system restart.

7. To connect the client through an HTTP proxy, enter the following command:

```
/opt/qradar/bin/vpntool client IP Address  /root/ca.crt
 /root/Console.p12 --http-proxy= IP Address:port
```

   - Proxy configuration is always in TCP mode, even if you do not enter TCP in the command.
   - See the OpenVPN documentation for configuration options for proxy authentication. Add these configuration options to the following file:

     `/etc/openvpn/client.conf`

Configuring a member for cloud installations

Use OpenVPN to establish secure connections for IBM Security QRadar hosts that are not servers or clients.

Procedure

To join a QRadar SIEM host to the local VPN, so that it communicates directly with hosts on the other side of the tunnel, by using the following command:

```
/opt/qradar/bin/vpntool join local_host_IP_address remote host IP address
/opt/qradar/bin/vpntool deploy
```

Chapter 9. Data Node Overview

Understand how to use Data Nodes in your IBM Security QRadar deployment.

Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required.

Users can scale storage and processing power independently of data collection, which results in a deployment that has the appropriate storage and processing capacity. Data Nodes are plug-n-play and can be added to a deployment at any time. Data Nodes seamlessly integrate with the existing deployment.

Increasing data volumes in deployments require data compression sooner. Data compression slows down system performance as the system must decompress queried data before analysis is possible. Adding Data Node appliances to a deployment allows you to keep data uncompressed longer.

The QRadar deployment distributes all new data across the Event and Flow processors and the attached Data Nodes.

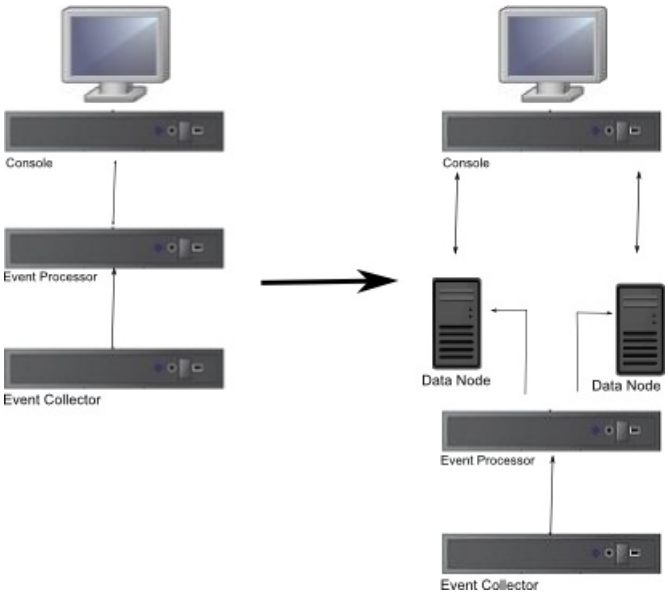

Figure 2. QRadar deployment before and after adding Data Node appliances

Clustering

Data Nodes add capacity to a deployment, but also improve performance by distributing data throughout the deployment. Queries are executed by many hosts, using the system resources of the entire cluster. Clustering allows searches that are multiple times faster than in a non-clustered approach.

Deployment Considerations

- Data Nodes are available on QRadar 7.2.2 and later
- Data Nodes perform similar search and analytic functions as Event and Flow processors in a QRadar deployment. Operations on a cluster are affected by the

slowest member of a cluster. Data Node system performance improves if Data Nodes are sized similarly to the event and flow processors in a deployment. To facilitate similar sizing between Data Nodes and event and flow processors, Data Nodes are available on both XX05 and XX28 core appliances.

- Data Nodes are available in three formats: Software (on your own hardware), Physical and Appliances. You can mix the formats in a single cluster.

Bandwidth and latency

Ensure a 1 Gbps link and less than 10 ms between hosts in the cluster.

Compatibility

Data Nodes are compatible with all existing QRadar appliances that have an Event or Flow Processor component, including All-In-One appliances. Data Nodes are not compatible with QRadar Incident Forensics PCAP appliances.

Data Nodes support high-availability (HA).

Installation

Data Nodes use standard TCP/IP networking, and do not require proprietary or specialized interconnect hardware. Install each Data Node that you want to add to your deployment as you would install any other QRadar appliance. Associate Data Nodes with event or flow processors in the QRadar Deployment Editor. See *IBM Security QRadar Administration Guide*.

You can attach multiple Data Nodes to a single Event or Flow Processor, in a many-to-one configuration.

When you deploy HA pairs with Data Node appliances, install, deploy and rebalance data with the High Availability appliances before synchronizing the HA pair. The combined effect of the data rebalancing and the replication process utilized for HA results in significant performance degradation. If High Availability is present on the existing appliances to which Data Nodes are being introduced, it is also preferable that the HA connection be broken and reestablished once the rebalance of the cluster is completed.

Decommissioning

Remove Data Nodes from your deployment with the Deployment Editor, as with any other QRadar appliance. Decommissioning does not erase balanced data on the host. You can retrieve the data for archiving and redistribution.

Data Rebalancing

Adding a Data Node to a cluster distributes data evenly to each Data Node. Each Data Node appliance maintains the same percentage of available space. New Data Nodes added to a cluster initiate additional rebalancing from cluster event and flow processors to achieve efficient disk usage on the newly added Data Node appliances.

Starting in QRadar 7.2.3, data rebalancing is automatic and concurrent with other cluster activity, such as queries and data collection. No downtime is experienced during data rebalancing.

Data Nodes offer no performance improvement in the cluster until data rebalancing is complete. Rebalancing can cause minor performance degradation during search operations, but data collection and processing continue unaffected.

Management and Operations

Data Nodes are self-managed and require no regular user intervention to maintain normal operation. QRadar manages activities, such as data backups, high-availability and retention policies, for all hosts, including Data Node appliances.

Failures

If a Data Node fails, the remaining members of the cluster continue to process data.

When the failed Data Node returns to service, data rebalancing can occur to maintain proper data distribution in the cluster, and then normal processing resumes. During the downtime, data on the failed Data Node is unavailable.

For catastrophic failures requiring appliance replacement or the reinstallation of QRadar, decommission Data Nodes from the deployment and replace them using standard installation steps. Copy any data not lost in the failure to the new Data Node before deploying. The rebalancing algorithm accounts for data existing on a data node, and shuffles only data collected during the failure.

For Data Nodes deployed with an HA pair, a hardware failure causes a failover, and operations continue to function normally.

Related concepts:

"QRadar components" on page 2
IBM Security QRadar consolidates event data from log sources that are used by devices and applications in your network.

Chapter 10. 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
- Confirm that there are no undeployed changes.
- If you are changing the IP address host name of a box in the deployment you must remove it from the deployment.
- If this system is part of an HA pair you must disable HA first before you change any network settings.
- If the system that you want to change is the console, you must remove all hosts in the deployment before proceeding.

Procedure

1. Log in to as the root user.
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 14. 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 as QRadar 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 multi-system deployment

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

Before you begin

- You must have a local connection to your QRadar Console

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 **System and License Management** icon.

   c. Select the managed host that you want to remove.

   d. Select **Deployment Actions** > **Remove Host**.

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

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 a multi-system 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.

4. To re-add 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 **System and License Management** icon.

c. Click **Deployment Actions** > **Add Host**.

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

   Select the **Network Address Translation** 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

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

   a. Click the **Admin** tab.

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

   c. Select the host that you want to reassign.

   d. Click **Deployment Actions** > **Edit Host Connection**.

   e. Enter the IP address of the source host in the **Modify Connection** window.

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`.

Chapter 11. 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 16. 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, tech notes, 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.

Related concepts:

"QRadar components" on page 2
IBM Security QRadar consolidates event data from log sources that are used by devices and applications in your network.

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.

Related concepts:

"QRadar log files" on page 53
Use the IBM Security QRadar log files to help you troubleshoot problems.

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.

Tech notes and APARs

From the IBM Support Portal (http://www.ibm.com/support/entry/portal), you can search tech notes 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:
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug
3. Review all logs by selecting **Admin** > **System & License Mgmt** > **Actions** > **Collect Log Files**.

Related concepts:

"Troubleshooting resources" on page 51
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.

Common ports and servers used by QRadar

Review the common ports that IBM Security QRadar services and components use to communicate across the network. For example, you can determine the ports that must be opened for the QRadar Console to communicate with remote Event Processors.

This chapter documents the listening ports for QRadar. The listen ports are valid only when iptables is enabled on your QRadar system.

SSH communication on port 22

All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by using encryption, through port 22 over SSH. For security reasons, you cannot set up an SSH tunnel from the managed host to the console, but you can set up an SSH tunnel from the console to the managed host. The managed host's public key is not added to the console's authorized keys file. These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event

Processor appliances 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.

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.

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 information on all listening ports, type the following command:

     ```
     netstat -nap | grep LISTEN
     ```

Viewing IMQ port associations

Several ports used by IBM Security QRadar allocate additional random port numbers. For example, Message Queues (IMQ) open random ports for communication between components on a managed host. You can view the random port assignments for IMQ using telnet to connect to the localhost and doing a look up on the port number.

Random port associations are not static port numbers. If a service is restarted, the ports generated for the service are reallocated and the service is provided with a new set of port numbers.

Procedure

1. Using SSH, 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
   telnet localhost 7677
   ```
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 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.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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