IBM Security QRadar SIEM
Version 7.1.0 (MR2)

Installation Guide

IBM

Note: Before using this information and the product that it supports, read the information in "Notices and Trademarks" on page 43.

CONTENTS

6 Network settings management

A Notices and Trademarks

Index

ABOUT THIS GUIDE

The *IBM Security QRadar SIEM Installation Guide* provides you with QRadar SIEM 7.1 (MR2) installation procedures. QRadar SIEM appliances are pre-installed with software and a Red Hat Enterprise Linux version 6.3 operating system. You can also install QRadar SIEM software on your own hardware.

This guide does not cover installation and recovery of High Availability (HA) systems. If you want to install or recover an HA system, see the *IBM Security QRadar High Availability Guide*.

Intended audience

This guide is intended for network administrators responsible for installation and configuration of QRadar SIEM systems in your network. This guide assumes a working knowledge of networking and Linux systems.

Documentation conventions

The following conventions are used throughout this guide:

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

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

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

Technical documentation

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

Contacting customer support

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

Statement of good security practices

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

1 PREPARATION FOR YOUR INSTALLATION

To ensure a successful QRadar SIEM deployment, adhere to the preparation requirements and recommendations included in this topic.

QRadar SIEM deployment overview

QRadar SIEM deployment architecture allows you to install components on a single server for small enterprises or distributed across multiple servers for maximum performance and scalability in large enterprise environments.

QRadar SIEM also provides High Availability (HA) functionality, which requires you to install redundant appliances for each system that requires HA protection. If you want to install or recover an HA system, see the *QRadar High Availability Guide*.

QRadar SIEM components

QRadar SIEM deployments can include the following components:

- **QRadar QFlow Collector** - Passively collects traffic flows from your network through span ports or network taps. The 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.
- **Console** - Provides the QRadar SIEM user interface, which provides real time event and flow views, reports, offenses, asset information, and administrative functionality. Using the Console, you can also manage hosts that include other components in a distributed QRadar SIEM deployment.
- **Event Collector** - Gathers events from local and remote log sources. The Event Collector normalizes raw log source events. During this process, the Magistrate component examines the event from the log source and maps the event to a QRadar Identifier (QID). Then the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.
- **Event Processor** - Processes events collected from one or more Event Collector. The Event Processor correlates the information from QRadar SIEM and distributes the information to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by QRadar SIEM to indicate behavioral changes or policy violations for the event. When complete, the Event Processor sends the events to the Magistrate component.

- **Magistrate** - Provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes events against the custom rules. If an event matches a rule, the magistrate generates the response configured in the custom rule. For example, the custom rule may indicate that when an event matches the rule, an offense is created. If there is no match to a custom rule, the Magistrate uses default rules to process the event. An offense is an alert that has been processed using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. The magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility.

For more information on each QRadar SIEM component, see the *IBM Security QRadar SIEM Administration Guide*.

Additional hardware requirements

Before you install QRadar SIEM systems, make sure 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 Consoles, Event Processors, or QRadar QFlow Collectors
- Null modem cable if you want to connect the system to a serial console

Additional software requirements

Before you install QRadar SIEM, make sure you have the following applications installed on any desktop system that you use to access the QRadar SIEM user interface:

- Java^{TM} Runtime Environment (JRE)
- Adobe Flash 10.x

You can download Java 1.6.0_u24 at the following website: *http://java.com/*. Make sure that you install JRE on your desktop system, not on the QRadar SIEM system.

Supported browsers

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

Table 1-1 Supported web browsers

Web browser	Supported versions
Mozilla Firefox	• 10.0 Due to Mozilla's short release cycle, we cannot commit to test the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigate any issues that are reported.
Microsoft Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0 For instructions on how to enable Compatibility View, see **Enabling Compatibility View for Microsoft Internet Explorer**.

Enabling Compatibility View for Microsoft Internet Explorer

To use the Microsoft Internet Explorer web browser, you must enable Compatibility View.

Procedure

Step 1 Press F12 to open the Developer Tools window.

Step 2 Configure the following compatibility settings:

Table 1-2 Microsoft Internet Explorer Compatibility Settings

Browser Version	Option	Description
Microsoft Internet Explorer 8.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 8.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**
Microsoft Internet Explorer 9.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 9.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**

Required network settings

Before you install QRadar SIEM, you must identify the following information for each system that you want to install:

- Hostname
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server address (optional)

- Public IP address for networks using Network Address Translation (NAT)
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

2 QRADAR SIEM CONSOLE AND MANAGED HOST INSTALLATION

Use the procedures in this topic to install QRadar SIEM Consoles and managed host appliances (non-Consoles). QRadar SIEM appliances include QRadar SIEM software and a Red Hat Enterprise Linux operating system. You can also install QRadar SIEM software on your own hardware.

For more information about appliances, see the *Hardware Installation Guide*.

Preparing your QRadar SIEM appliance for installation

Before you can use the installation wizard to install a QRadar SIEM appliance, you must physically install and prepare the appliance.

About this task

If you use a laptop to connect to the system, you must use a terminal program, such as HyperTerminal, to connect to the system. Make sure you set **Connect Using** to the appropriate COM port of the serial connector and **Bits per second** to 9600. You must also set **Stop Bits** (1), **Data bits** (8), and **Parity** (None).

For more information on your QRadar SIEM appliance, see the *Hardware Installation Guide*.

Procedure

Step 1 Install all necessary hardware.

Step 2 Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.
- Connect a keyboard and monitor to their respective ports.

Step 3 Power on the system and log in:

Username: **root**

Note: The username is case sensitive.

Step 4 Press Enter.

What to do next

Installing a QRadar SIEM Console or managed host

Preparing your own appliance for installation

You can install QRadar SIEM software on your own hardware using the Red Hat Enterprise Linux 6.3 operating system. Before you can install QRadar SIEM software on your own appliance, you must prepare your appliance.

About this task

Red Hat Enterprise Linux 6.3 operating system is a vendor system. For more information on how to install the Red Hat Linux 6.3 operating system, see your vendor documentation. For QRadar SIEM specific guidelines on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing the Red Hat Enterprise Linux operating system**.

Procedure

Step 1 Install the necessary hardware.

Step 2 Obtain the Red Hat Enterprise Linux 6.3 operating system and install it on your hardware.

Step 3 Log in as the root user.

Username: **root**

Note: The username is case sensitive.

Step 4 To create the /media/cdrom redhat directory, type the following command:

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the support website *http://www.ibm.com/support*.

Step 6 To mount the QRadar SIEM 7.1 (MR2) ISO, type the following command:

```
mount -o loop <path to the QRadar SIEM ISO> /media/cdrom
```

Step 7 To begin the installation, type the following command:

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

What to do next

Installing a QRadar SIEM Console or managed host

Installing a QRadar SIEM Console or managed host

Use this procedure to install a QRadar SIEM Console or managed host. You can also use this procedure to install QRadar SIEM software on your own appliance.

Before you begin

Before you begin, ensure that the following requirements are met:

- Your appliance is prepared for installation. If your appliance is not prepared for installation, choose one of the following:
  - **Preparing your QRadar SIEM appliance for installation**
  - **Preparing your own appliance for installation**
- The End User License Agreement (EULA) window is displayed.

- Locate your activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM. The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

About this task

When you read the End User License Agreement (EULA), press the Spacebar to advance each window until you reach the end of the document.

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

When you create the root password, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

Procedure

Step 1 Read the information in the End User License Agreement (EULA) window.

Step 2 Type **yes** to accept the agreement, and then press Enter.

Step 3 Type your activation key and press Enter.

Step 4 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 5 If you are installing a non-Console appliance, go to **Step 8**.

Step 6 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 7 Configure your time settings:

a Choose one of the following options:

- **Manual** - Select this option to manually input the time and date. Select **Next** and press Enter. The Current Date and Time window is displayed. Go to **b**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **c**.

b To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 8**.

c To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter. Go to **Step 10**.

Step 8 On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

Step 9 On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

Step 10 Select an internet protocol version. Select **Next** and press Enter.

Step 11 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 12 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 15**.
- If you use IPv6 as your Internet protocol, go to **Step 13**.

Step 13 Choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 15**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 14**.

Step 14 Enter network information to use for IPv6:

a In the **Hostname** field, type a fully qualified domain name as the system hostname.

b In the **IP Address** field, type the IP address of the system.

c In the **Email server** field, type the email server. If you do not have an email server, type `localhost` in this field.

d Select **Next** and press Enter. Go to **Step 16**

Step 15 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 16 Configure the QRadar SIEM root password:

a Type your password. Select **Next** and press Enter.

b Retype your new password to confirm. Select **Finish** and press Enter.

Step 17 Press Enter to select **OK**.

Result

After you configure the installation parameters, a series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

What to do next

See **Accessing the QRadar SIEM user interface**.

Accessing the QRadar SIEM user interface

After the installation is complete, you can access the QRadar SIEM user interface.

About this task

When you access the QRadar SIEM for the first time, note the following requirements:

- If you use Mozilla Firefox, you must add an exception to Mozilla Firefox. For more information, see your Mozilla documentation.
- If you use Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar SIEM.
- For your QRadar SIEM Console, a default license key provides you access to QRadar SIEM for five weeks. For more information on the license key, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar SIEM:

`https://<IP Address>`

Where <**`IP Address`**> is the IP address of the QRadar SIEM system. The default values are:

Username: **`admin`**

Password: **`<root password>`**

Step 3 Click **Login To QRadar SIEM**.

3 INSTALLING THE RED HAT ENTERPRISE LINUX OPERATING SYSTEM

Use this task to install the Red Hat Enterprise Linux 6.3 operating system on your own appliance for use with IBM Security QRadar SIEM.

Before you begin

Before you install the Red Hat Enterprise Linux 6.3 operating system, note the following:

- QRadar SIEM supports the 64-bit versions of the Red Hat Enterprise Linux 6.3 operating system.
- QRadar SIEM does not support KickStart disks. These disks may cause the application to install incorrectly.
- If you want to use NTP as your time server, make sure you install the NTP package. For more information, see your Red Hat documentation.
- For Console systems, must have at least 8 GB of RAM and at least 256 GB of free disk space.
- If you plan to enable payload indexing we strongly recommend that your Console has at least 24 GB of RAM. We require that you upgrade your system memory before you install QRadar SIEM on your system.
- For QRadar QFlow Collectors, make sure the primary drive is at least 70 GB of free space.
- The firewall configuration must allow WWW (http, https) and SSH traffic. Before you configure the firewall, disable the SELinux option. The QRadar SIEM installation includes a default firewall template, which you can update in the System Setup window.

About this task

If you want to delete and recreate partitions rather than edit the default partitions, use the following table as a guide:

Table 1-1 Partition guide

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/boot	System boot files	/boot	EXT4	101 MB	Yes	SDA
swap	Area to be used as memory when RAM is full.	empty	swap	For systems with 4 to 8 GB of RAM, the size of the swap partition must match the amount of RAM, For 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
/	Install area for QRadar SIEM, the operating system, and associated files.	/	EXT4	20000 MB	No	SDA
/store/tmp	Storage area for QRadar SIEM temporary files	/store/tmp	EXT4	20000 MB	No	SDA
/var/log	Storage area for QRadar SIEM and system log files	/var/log	EXT4	20000 MB	No	SDA
/store	Storage area for all QRadar SIEM data and configuration files	/store	EXT4	Select the **Fill to maximum allowable size** check box	No	SDA

Note: If an error is displayed when the software RAID partitions are created, contact Customer Support.

CAUTION: *Future software upgrades will fail if you reformat any of the following partitions or their sub-partitions: /store, /store/tmp, /store/ariel, /store/persistent data.*

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

- **/store** as **RAID5** - Stores QRadar SIEM data. Choose **EXT4** as the file system type.
- **FLOWLOGS** and **DB** are located in the **Store** partition. In a system with five drives, a suggested configuration includes:
  - **disk 1** - boot, swap, OS, QRadar SIEM temporary files, and log files
  - **remaining disks** - RAID 5, mounted as **/store**

Note: Other QRadar SIEM components do not require the storage partitions mentioned above.

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

Procedure

Step 1 Install the Red Hat Enterprise Linux 6.3 operating system:

a Obtain the Red Hat Enterprise Linux 6.3 operating system DVD ISO and copy the ISO to one of the following portable storage devices:

- Digital Versatile Disk (DVD)
- Bootable USB flash-drive

  For instructions on how to create a bootable USB flash-drive, see the *Installing QRadar Using a Bootable USB Flash-Drive Technical Note*.

b Insert the portable storage device into your appliance.

c Restart your appliance.

d Load the boot menu.

e Choose one of the following options:

- Select the USB drive or DVD drive as the boot option.
- To install the Red Hat Enterprise Linux operating system on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode. Select **boot from legacy dvd** or **boot from legacy usb**.

f When the login prompt is displayed, log in to the system as the root user.

Step 2 To prevent an issue with ethernet interface address naming, perform the following steps on the Welcome page:

a Press the Tab key.

b Locate the following line:

```
Vmlinuz initrd=initrd.image
```

c At the end of the `Vmlinuz initrd=initrd.image` line, add the following text:

```
biosdevname=0
```

d To return to the installation wizard, press Enter.

Step 3 Click **Next** to advance to the next page.

Step 4 Select the language that you want to use for the installation process and as the system default. Click **Next**.

Step 5 Select the type of keyboard layout that you want to use. Click **Next**.

Step 6 Select the **Basic Storage Devices** option. Click **Next**

Step 7 In the **Hostname** field, type a unique name of your server.

The host name can include letters, numbers, and hyphens.

Step 8 Click **Configure Network**.

The Network Connections window is displayed.

Step 9 Select **System eth0**. Click **Edit**.

Step 10 Configure the parameters:

- **a** Select the **Connect automatically** check box.
- **b** Click the **IPv4 Settings** tab.
- **c** From the **Method** list box, select **Manual**.
- **d** In the Addresses pane, click **Add**, and then add the IP, Netmask, and Gateway addresses for your server.
- **e** In the **DNS servers** field, type a comma-separated list of DSN servers.
- **f** Click **Apply**.
- **g** Click **Close**.

Step 11 Click **Next** to advance to the next page.

Step 12 From the list box, select a time zone. Click **Next**.

Step 13 Configure your root password for your system:

- **a** In the **Root Password** field, type a root password.
- **b** In the **Confirm** field, type the root password again.
- **c** Click **Next** to advance to the next page.

Step 14 Select the **Create Custom Layout** option. Click **Next**.

Step 15 Configure disk partitioning:

- **a** Configure the mount points for each disk partition.
- **b** For all other partitions, such as /, /boot, and /var/log, configure the file system type to be EXT4.
- **c** Reformat the swap partition with a file system type of swap. For important information on partition requirements, see **About this task**.

Step 16 Click **Next**. No changes are required on this page.

Step 17 Click **Next**.

Step 18 Select the **Basic Server** option. Click **Next**.

Step 19 When the installation is complete, click **Reboot**.

What to do next

Installing a QRadar SIEM Console or managed host

4 RE-INSTALLATION FROM THE RECOVERY PARTITION

If required, you can re-install IBM Security QRadar SIEM software from the recovery partition. This section applies to new QRadar SIEM 7.1 (MR2) installations or upgrades from new QRadar SIEM 7.0 installations on QRadar SIEM appliances.

Recovery partition overview

When you install QRadar SIEM, the installer (ISO) is copied into the recovery partition. From this partition, you can re-install QRadar SIEM, which restores QRadar SIEM to factory defaults. Your system is restored back to factory default configuration. Your current configuration and data files are overwritten.

When you reboot your QRadar SIEM appliance, you are presented with the option to re-install the software. If you do not respond to the prompt after 5 seconds, the system reboots as normal, thus your configuration and data files are maintained. If you choose the re-install QRadar SIEM option, a warning message is displayed and you must confirm that you want to re-install QRadar SIEM. After confirmation, the installer runs and you can follow the prompts through the installation process.

Note: After a hard disk failure, you are unable to re-install from the recovery partition, because it is longer be available. If you experience a hard disk failure, contact Customer Support for assistance.

Any software upgrades you perform after you install QRadar SIEM 7.1 (MR2) replaces the ISO file with the newer version.

Re-installing QRadar SIEM from the recovery partition

This topic provides the procedure for re-installing QRadar SIEM from the recovery partition.

Before you begin

Before you begin, ensure that the following requirements are met:

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

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

If you do not have your activation key, contact the Welcome Center at *q1pd@us.ibm.com* or or *http://www.ibm.com/support* with the serial number of the QRadar SIEM appliance. Software activation keys do not require serial numbers

About this task

When you read the End User License Agreement (EULA), press the Spacebar to advance each window until you reach the end of the document.

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

When you create the root password, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

When you type `flatten` during the procedure, the installer partitions and reformats the hard disk, installs the OS, and then re-installs QRadar SIEM. You must wait for the flatten process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.

Procedure

Step 1 Reboot your QRadar SIEM appliance.

Step 2 Select **Factory re-install**.

Step 3 Type `flatten` to continue.

Step 4 Type `SETUP`.

Step 5 Log in to QRadar SIEM as the root user.

Username: root

Password: <password>

Step 6 Read the information in the End User License Agreement (EULA) window.

Step 7 Type your activation key and press Enter.

Step 8 If you are re-installing a non-Console appliance, go to **Step 11**.

Step 9 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 10 Configure your time settings:

a Choose one of the following options:

- **Manual** - Select this option to manually input the time and date. Select **Next** and press Enter. The Current Date and Time window is displayed. Go to **b**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **c**.

b To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 11**.

c To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter. Go to **Step 13**.

Step 11 On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

Step 12 On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

Step 13 Select an internet protocol version. Select **Next** and press Enter.

Step 14 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 15 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 18**.
- If you use IPv6 as your Internet protocol, go to **Step 16**.

Step 16 Choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 18**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 17**.

Step 17 Enter network information to use for IPv6:

a In the **Hostname** field, type a fully qualified domain name as the system hostname.

b In the **IP Address** field, type the IP address of the system.

c In the **Email server** field, type the email server. If you do not have an email server, type `localhost` in this field.

d Select **Next** and press Enter. Go to **Step 19**.

Step 18 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.

- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 19 Configure the QRadar SIEM root password:

a Type your password. Select **Next** and press Enter

The password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

The Confirm New Root Password window is displayed.

b Retype your new password to confirm. Select **Finish** and press Enter.

Step 20 Press Enter to select **OK**.

Result

After you configure the installation parameters, a series of messages are displayed as QRadar SIEM continues with the re-installation. This process typically takes several minutes.

What to do next

See **Accessing the QRadar SIEM user interface**

Accessing the QRadar SIEM user interface

After the installation is complete, you can access the QRadar SIEM user interface.

About this task

When you access the QRadar SIEM for the first time, note the following requirements:

- If you use Mozilla Firefox, you must add an exception to Mozilla Firefox. For more information, see your Mozilla documentation.
- If you use Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar SIEM.
- For your QRadar SIEM Console, a default license key provides you access to QRadar SIEM for five weeks. For more information on the license key, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar SIEM:

`https://<IP Address>`

Where <**`IP Address`**> is the IP address of the QRadar SIEM system. The default values are:

Username: **`admin`**

Password: **`<root password>`**

Step 3 Click **Login To QRadar SIEM**.

5 VIRTUAL APPLIANCE INSTALLATION

A virtual appliance is a QRadar SIEM system that consists of QRadar SIEM software installed on a VMWare ESX 5.0 virtual machine. Use the procedures in this topic to install your virtual appliance.

Virtual appliance overview

A virtual appliance enables the same visibility and functionality in your virtual network infrastructure that QRadar SIEM appliances offer in your physical environment.

After you install your virtual appliances, you can access the deployment editor and add your virtual appliances to your deployment. For more information on how to connect appliances, see the *IBM Security QRadar SIEM Administration Guide*.

The following virtual appliances are available:

- **QRadar SIEM 3190** - The QRadar SIEM 3190 virtual appliance is a QRadar SIEM system that can profile network behavior and identify network security threats. The QRadar SIEM 3190 virtual appliance includes an on-board Event Collector and internal storage for events. The QRadar SIEM 3190 virtual appliance supports:
    - Up to 1,000 network objects
    - 50,000 flows per interval, depending on your license
    - 1,000 Events Per Second (EPS), depending on your license
    - 750 event feeds (additional devices can be added to your licensing)
    - External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
    - QRadar QFlow Collector and Layer 7 network activity monitoring

You can also add one or more of the following virtual appliances to expand the capacity of the QRadar SIEM 3190 beyond license-based upgrade options:

  - QRadar SIEM 1690
  - QRadar SIEM 1790

- **QRadar SIEM 1690** - The QRadar SIEM 1690 virtual appliance is a dedicated Event Processor that allows you to scale your QRadar SIEM deployment to manage higher EPS rates. The QRadar SIEM 1690 includes an on-board Event Collector, Event Processor, and internal storage for events. The QRadar SIEM 1690 appliance supports:
  - Up to 1,000 events per second
  - 2 TB or larger dedicated event storage
  - The QRadar SIEM 1690 virtual appliance is a distributed Event Processor appliance and requires a connection to any QRadar SIEM 3105 or 3124 series appliance
- **QRadar SIEM 1790** - The QRadar SIEM 1790 virtual appliance is deployed in conjunction with any QRadar SIEM 3105 or 3124 series appliance to increase storage. The QRadar SIEM 1790 virtual appliance includes an on-board Event Processor, and internal storage. The QRadar SIEM 1790 appliance supports:
  - 50,000 flows per interval depending on traffic types
  - 2 TB or larger dedicated flow storage
  - 1,000 network objects
  - You can add QRadar SIEM 1790 appliances to any QRadar SIEM 3105 or 3124 series appliance to increase your deployment’s storage and performance.
  - QRadar QFlow Collector and Layer 7 network activity monitoring
- **QRadar VFlow Collector** - The QRadar VFlow Collector virtual appliance provides the same visibility and functionality in your virtual network infrastructure that a QRadar QFlow Collector offers in your physical environment. The QRadar VFlow 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 virtual appliance supports a maximum of:
  - 10,000 flows per minute
  - Three virtual switches, with one additional switch that is designated as the management interface.

  The QRadar VFlow Collector 1290 virtual appliance does not support NetFlow.
- **QRadar SIEM 1590** - The QRadar SIEM 1590 virtual appliance is a dedicated event collector, which is required if you want to enable the Store and Forward feature. The Store and Forward feature allows you to manage schedules that control when to start and stop forwarding events from your dedicated Event Collector appliances to Event Processors in your deployment. A dedicated Event Collector does not process events and it does not include an on-board

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

Virtual appliance requirements

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

- Virtual appliances require VMware ESXi 5.0. You must have a VMware client installed on your desktop. VMware server applications are bundled with client software. For example, ESXi 5.0 is bundled with VMware vSphere client 5.0. If your server/client configuration differs, we recommend you upgrade your VMware server and client. For more information, see *http://www.vmware.com*.
- 4 GB of free memory is required by the VMware host for QRadar SIEM 1690 and QRadar SIEM 1790. 12 GB is optimal.
- 8 GB of free memory is required by the VMware host for QRadar SIEM 3190. 12 GB is optimal.
- 256 GB of free disk space is required on all virtual appliance types except QRadar QFlow Collectors.
- QRadar QFlow Collectors require at least 70 GB of free disk space.

Virtual appliance installation procedures

The process to install a virtual appliance includes the following tasks, which must be performed in sequence.

1. **Creating your virtual machine**
2. **Installing the QRadar SIEM ISO on the virtual machine**
3. **Installing QRadar SIEM software on your virtual machine**
4. **Adding your virtual appliance to your deployment**

Creating your virtual machine

To install a virtual appliance, you must first create a virtual machine using VMware vSphere client 5.0.

About this task

When you configure the parameters on the CPU page, you must configure a minimum of two processors. The combination of number of virtual sockets and number of cores per virtual socket determines how many processors are configured on your system. The following table provides examples of CPU page settings you can use:

Table 1-2 Sample CPU page settings

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

Procedure

Step 1 Access your vSphere Client.

Step 2 Select **File > New > Virtual Machine**.

Step 3 In the Configuration pane of the Create New Virtual Machine window, select the **Custom** option and click **Next**.

Step 4 In the **Name** field, type a unique name for the virtual machine and click **Next**.

Step 5 In the right pane, select the datastore where you want to store the virtual machine and click **Next**.

Step 6 In the Virtual Machine Version pane, select the **Virtual Machine Version: 7** option and click **Next**.

Step 7 Select the Operating System (OS) for the QRadar SIEM virtual appliance:

a In the Guest Operating System pane, select the **Linux** option.

b From the **Version** list box, select **Red Hat Enterprise Linux 6 (64-bit)** and click **Next**.

Step 8 On the CPUs page, configure the number of virtual processors that you want for the virtual machine:

a From the **Number of virtual sockets** list box, select the number of sockets that you want for the virtual machine and click **Next**.

b From the **Number of cores per virtual socket** list box, select the number of sockets that you want for the virtual machine and click **Next.**

Step 9 In the Memory Configuration pane, provide a minimum of 8 GB for memory:

a In the **Memory Size** field, type or select **8** or higher.

b In the list box, select **GB**.

Step 10 Configure your network connections:

a From the **How many NICs do you want to connect** list box, select the number of Network Interface Controllers (NICs) that you want to add. You must add at least one NIC.

b For all NICs, select **VMXNET3** from the **Adapter** list box.

c Click **Next**.

Step 11 In the SCSI controller pane, select **VMware Paravirtual** and click **Next**.

Step 12 In the Disk pane, select **Create a new virtual disk**.

Step 13 Configure the virtual disk size and specify a provisioning policy:

a In the Capacity pane, type or select 256 or higher and select **GB** from the list box.

b In the Disk Provisioning pane, select the **Thin provision** check box.

c Click **Next**.

The Advanced Options page is displayed. Do not configure the options on this page.

Step 14 Click **Next**.

Step 15 On the Ready to Complete page, review the settings and click **Finish**.

What to do next

Installing the QRadar SIEM ISO on the virtual machine

Installing the QRadar SIEM ISO on the virtual machine

After you create your virtual machine, you must install the QRadar SIEM ISO on the virtual machine.

Before you begin

Before you begin, ensure that you created a virtual machine. See **Creating your virtual machine**.

Procedure

Step 1 Obtain the QRadar SIEM software from the support website *http://www.ibm.com/support*.

Step 2 In the left pane of your VMware vSphere Client, select your virtual machine from the menu tree.

Step 3 In the right pane, click the **Summary** tab.

Step 4 In the Commands pane, click **Edit Settings**.

Step 5 In the left pane of the Virtual Machine Properties window, click **CD/DVD Drive 1**.

Step 6 In the Device Status pane, select the **Connect at power on** check box.

Step 7 In the Device Type pane, select **Datastore ISO File** and click **Browse**.

is displayed.

Step 8 On the Browse Datastores window, locate and select the ISO file and click **Open**.

Step 9 Click **OK**.

What to do next

Installing QRadar SIEM software on your virtual machine.

Installing QRadar SIEM software on your virtual machine

After your virtual machine is configured and QRadar SIEM ISO is installed, power on and continue the QRadar SIEM software installation.

Before you begin

Before you begin, you must have created a virtual machine and installed the QRadar SIEM ISO on the machine. See the following topics:

- **Creating your virtual machine**
- **Installing the QRadar SIEM ISO on the virtual machine**

You must also locate your activation key. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM. The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

About this task

When you read the End User License Agreement (EULA), press the Spacebar to advance each window until you reach the end of the document.

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

When you create the root password, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

Procedure

Step 1 Access your vSphere Client.

Step 2 In the menu tree, right-click your virtual machine and select **Power > Power On**.

Step 3 Log in to the virtual machine:

Username: **root**

Note: The username is case sensitive.

Step 4 Press Enter.

Step 1 Read the information in the End User License Agreement (EULA) window.

Step 2 Type **yes** to accept the agreement, and then press Enter.

Step 3 Type your activation key and press Enter.

Step 4 Select **normal** for your type of setup. Select **Next** and press Enter.

Step 5 Specify if you want to install a Console or non-Console system.

- **Yes** - Select this option if this system is a Console.
- **No** - Select this option if this system is not a Console.

Step 6 Select **Next** and press Enter.

Step 7 If you are installing a non-Console appliance, go to **Step 10**.

Step 8 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 9 Configure your time settings:

a Choose one of the following options:

- **Manual** - Select this option to manually input the time and date. Select **Next** and press Enter. The Current Date and Time window is displayed. Go to **b**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **c**.

b To manually enter the time and date, type the current time and date. Select **Next** and press Enter. Go to **Step 10**.

c To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter. Go to **Step 10**.

Step 10 On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

Step 11 On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

Step 12 Select an internet protocol version. Select **Next** and press Enter.

Step 13 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 14 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 17**.
- If you use IPv6 as your Internet protocol, go to **Step 15**.

Step 15 Choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 17**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 16**.

Step 16 Enter network information to use for IPv6, type the values for the **Hostname** and **Email server**. Select **Next** and press Enter.

Step 17 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 18 Configure the QRadar SIEM root password:

a Type your password. Select **Next** and press Enter**.**

b Retype your new password to confirm. Select **Finish** and press Enter.

c Press Enter to select **OK**.

Result

After you configure the installation parameters, a series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

What to do next

Adding your virtual appliance to your deployment

Adding your virtual appliance to your deployment

After your virtual appliance is installed, you must add the virtual appliance to your deployment using the deployment editor.

Before you begin

Before you begin, you must have created a virtual machine, installed the QRadar SIEM ISO on the machine, and installed QRadar SIEM.

See the following topics:

- **Creating your virtual machine**
- **Installing the QRadar SIEM ISO on the virtual machine**
- **Installing QRadar SIEM software on your virtual machine**

About this task

The name you assign to the virtual appliance can be up to 20 characters in length and can include underscores or hyphens.

Procedure

Step 1 Log in to the QRadar SIEM Console.

Step 2 On the **Admin** tab, click **Deployment Editor**.

Step 3 In the Event Components pane on the Event View page, select the virtual appliance component that you want to add.

Step 4 On the first page of the Adding a New Component wizard, type a unique name for the virtual appliance. Click **Next**.

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

Step 6 Click **Finish**.

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

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

Accessing the QRadar SIEM user interface

After the installation is complete, you can access the QRadar SIEM user interface.

About this task

When you access the QRadar SIEM user interface for the first time, note the following requirements:

- If you use Mozilla Firefox, you must add an exception to Mozilla Firefox. For more information, see your Mozilla documentation.
- If you use Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar SIEM.
- For your QRadar SIEM Console, a default license key provides you access to QRadar SIEM for five weeks. For more information on the license key, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

Step 1 Open your web browser.

Step 2 Log in to QRadar SIEM:

```
https://<IP Address>
```

Where <`IP Address`> is the IP address of the QRadar SIEM system. The default values are:

Username: `admin`

Password: `<root password>`

Step 3 Click **Login To QRadar SIEM**.

6 NETWORK SETTINGS MANAGEMENT

Use the **`qchange_netsetup script`** to change the network settings of your QRadar SIEM system. Configurable network settings include hostname, IP address, network mask, gateway, DNS addresses, public IP address, and email server.

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

You can change the network settings in your all-in-one system. An all-in-one system has all QRadar SIEM components, including the **Admin** tab, installed on one system.

Before you begin

You must have a local connection to your Console before you start this procedure.

About this task

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

Procedure

Step 1 Log in to QRadar SIEM as the root user:

Username: root

Password: <password>

Step 2 Type the following command:

```
qchange_netsetup
```

Step 3 Select an internet protocol version. Select **Next** and press Enter.

Step 4 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 5 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 8**.
- If you use IPv6 as your Internet protocol, go to **Step 6**.

Step 6 To configure IPv6, choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 8**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 7**.

Step 7 Enter network information to use for IPv6:

a Type the values for the **Hostname**, **IP Address**, and **Email server**.

b Select **Next** and press Enter.

Step 8 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the name of the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 9 Select **Finish** and press Enter.

Result

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

Changing the network settings of a Console in a multi-system deployment

To change the network settings in a multi-system deployment, you must remove all managed hosts from the deployment, change the network settings, re-add the managed hosts, and then re-assign the component or components.

About this task

This procedure requires you to use the deployment editor. For more information on how to use the deployment editor, see the *IBM Security QRadar SIEM Administration Guide*.

You must perform this procedure in the following order:

1. **Removing managed hosts**
2. **Changing the network settings**
3. **Re-adding and re-assigning managed hosts**

Removing managed hosts

Before you can change network settings on a Console in a multi-system deployment, you must remove all managed hosts from your deployment.

Procedure

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where <`IP Address`> is the IP address of the QRadar SIEM system.

Username: **admin**

Password: **<admin password>**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Editor** icon.

Step 4 On the deployment editor window, click the **System View** tab.

Step 5 For each managed host in your deployment, right-click the managed host and select **Remove host**.

Step 6 Click **Save**.

Step 7 Close the deployment editor.

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

What to do next

Changing the network settings

Changing the network settings

After you remove all managed hosts from your Console, you can change the network settings on the Console.

Before you begin

Before you can change network settings on Console in a multi-system deployment, you must remove all managed hosts from your Console. See **Removing managed hosts**.

About this task

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

Procedure

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

Username: **root**

Password: **<password>**

Step 2 Type the following command:

```
qchange_netsetup
```

Step 3 Select an internet protocol version. Select **Next** and press Enter.

Step 4 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 5 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 8**.
- If you use IPv6 as your Internet protocol, go to **Step 6**.

Step 6 To configure IPv6, choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 8**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 7**.

Step 7 Enter network information to use for IPv6:

a Type the values for the **Hostname**, **IP Address**, and **Email server**.

b Select **Next** and press Enter.

Step 8 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the name of the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 9 Select **Finish** and press Enter.

Result

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

What to do next

Re-adding and re-assigning managed hosts

Re-adding and re-assigning managed hosts

After you remove all managed hosts from your Console and change the Console network settings, you must re-add and re-assign the managed hosts.

About this task

When you create the password for each managed host, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

Procedure

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where `<IP Address>` is the IP address of the QRadar SIEM system.

Username: **admin**

Password: **<admin password>**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Edit** icon.

The deployment editor is displayed.

Step 4 Click the **System View** tab.

Step 5 From the menu, select **Actions > Add a managed host**.

Step 6 On the Add a new host wizard, click **Next**.

Step 7 On the Enter the host’s IP window, enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of the host that you want to add to your System View.
- **Enter the root password of the host** - Type the root password for the host.
- **Confirm the root password of the host** - Type the password again, for confirmation.
- **Host is NATed** - Optional. Select this option to enable encryption.

Step 8 Click **Next**.

Step 9 Click **Finish**.

Step 10 Re-assign all components to your non-Console managed host.

- **a** In the QRadar SIEM deployment editor, click the **Event View** tab.
- **b** Select the component that you want to re-assign to the managed host.
- **c** From the menu, select **Actions > Assign**
- **d** From the **Select a host** list box, select the host that you want to re-assign to this component. Click **Next**.
- **e** Click **Finish**.

Step 11 Repeat for each non-Console managed host until all hosts are re-added and re-assigned.

Step 12 Close the deployment editor.

Step 13 Click **Deploy Changes**.

Changing the network settings of a managed host in a multi-system deployment

To change the network settings of a managed host in a multi-system deployment, you must remove the managed host that you want to change from the deployment, change the network settings, re-add the managed host, and then re-assign the original components.

About this task

This procedure requires you to use the deployment editor. For more information on how to use the deployment editor, see the *IBM Security QRadar SIEM Administration Guide*.

You must perform this procedure in the following order:

1. **Removing the managed host from your deployment**
2. **Changing the network settings of a managed host**
3. **Re-adding and re-assigning the managed host**

Removing the managed host from your deployment

Before you can change network settings on a managed host in a multi-system deployment, you must remove the managed host from your deployment.

Procedure

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where <`IP Address`> is the IP address of the QRadar SIEM system.

Username: **admin**

Password: **<admin password>**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Editor** icon.

Step 4 Click the **System View** tab.

Step 5 Right-click the managed host that you want to delete to access the menu, select **Remove host**.

Step 6 Close the deployment editor.

Step 7 Click **Deploy Changes**.

What to do next

Changing the network settings of a managed host

Changing the network settings of a managed host

After you remove the managed host from your Console, you can change the network settings on the managed host.

Before you begin

Before you can change network settings on managed host in a multi-system deployment, you must remove the managed host from your Console. See **Removing the managed host from your deployment**.

About this task

The Internet Protocol Version window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

When you configure the network settings, you can configure a public IP address for the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured 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.

Procedure

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

Username: root

Password: <password>

Step 2 Type the following command:

```
qchange_netsetup
```

Step 3 Select an internet protocol version. Select **Next** and press Enter.

The window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.

Step 4 Select the interface that you want to use as the management interface. Select **Next** and press Enter.

Step 5 Choose one of the following options:

- If you use IPv4 as your Internet protocol, go to **Step 8**.
- If you use IPv6 as your Internet protocol, go to **Step 6**.

Step 6 To configure IPv6, choose one of the following options:

a To automatically configure for IPv6, select **Yes** and press Enter. The automatic configuration can take an extended period of time. Go to **Step 8**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 7**.

Step 7 Enter network information to use for IPv6:

a Type the values for the **Hostname**, **IP Address**, and **Email server**.

b Select **Next** and press Enter.

Step 8 Configure the QRadar SIEM network settings:

a Enter values for the following parameters:

- **Hostname** - Type a fully qualified domain name as the system hostname.
- **IP Address** - Type the IP address of the system.
- **Network Mask** - Type the network mask address for the system.
- **Gateway** - Type the default gateway of the system.
- **Primary DNS** - Type the primary DNS server address.
- **Secondary DNS** - Optional. Type the secondary DNS server address.
- **Public IP** - Optional. Type the Public IP address of the server.
- **Email Server** - Type the name of the email server. If you do not have an email server, type `localhost` in this field.

b Select **Next** and press Enter.

Step 9 Select **Finish** and press Enter.

Result

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

What to do next

Re-adding and re-assigning the managed host

Re-adding and re-assigning the managed host

After you remove the managed host from your Console and change the network settings, you must re-add and re-assign the managed host.

About this task

When you create the root password for each managed host, the password must meet the following criteria:

- Must contain at least five characters
- No spaces
- Can include the following special characters: @,#,^, and *.

Procedure

Step 1 Log in to QRadar SIEM:

`https://<IP Address>`

Where <`IP Address`> is the IP address of the QRadar SIEM system.

Username: **admin**

Password: **<admin password>**

Step 2 Click the **Admin** tab.

Step 3 Click the **Deployment Editor** icon.

Step 4 Click the **System View** tab.

Step 5 From the menu, select **Actions > Add a managed host**.

Step 6 Click **Next**.

Step 7 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Type the IP address of the host that you want to add to your System View.
- **Enter the root password of the host** - Type the root password for the host.
- **Confirm the root password of the host** - Type the password again, for confirmation.
- **Host is NATed** - Select this option if you want to specify NAT values if necessary.
- **Enable Encryption** - Select this option if you want to enable encryption.

Step 8 Click **Next**.

Step 9 Click **Finish**.

Step 10 Re-assign all components to your non-Console managed host.

a In the QRadar SIEM deployment editor, click the **Event View** tab.

b Select the component that you want to re-assign to the managed host.

c From the menu, select **Actions > Assign**.

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

e Click **Finish**.

Step 11 Close the deployment editor.

Step 12 On the **Admin** tab, click **Deploy Changes**.

Updating network settings after a NIC Replacement

If you perform a replacement of your integrated motherboard or stand-alone NICs, you must update your QRadar SIEM network settings to ensure your hardware remains operational.

About this task

This task involves the network settings file. The file displays one pair of lines for each NIC that has been installed and one pair of lines for each NIC that has been removed. You must remove the lines for the NIC that you removed and then rename the NIC that you installed.

Your network settings file may resemble the following example:

```
# 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"
```

Where **`NAME=″eth0″`** is the NIC that was replaced and **`NAME=″eth4″`** is the NIC that was installed.

Procedure

Step 1 Using SSH, log in to QRadar SIEM as the root user:

Username: **root**

Password: **<password>**

Step 2 Type the following command:

```
cd /etc/udev/rules.d/
```

Step 3 To edit the network settings file, type the following command:

```
vi 70-persistent-net.rules
```

Step 4 Remove the pair of lines for the NIC which has been replaced; **`NAME=″eth0″`**.

Step 5 Rename the **`Name=<eth>`** values for the newly installed NIC. For example, **`NAME="eth4"`** should be renamed to **`NAME="eth0"`**.

Step 6 Save and close the file.

Step 7 Type the following command:

```
reboot
```

A NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

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

IBM 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 *http://www.ibm.com/legal/copytrade.shtml*.

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

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

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

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

INDEX