IBM Security QRadar SIEM
Version 7.1.0 MR1

Installation Guide

IBM

Note: Before using this information and the product that it supports, read the information in "Notices and Trademarks" on page 81.

CONTENTS

ABOUT THIS GUIDE

1 PREPARING FOR YOUR INSTALLATION

2 INSTALLING QRADAR SIEM APPLIANCES

3 INSTALLING QRADAR SIEM SOFTWARE ON YOUR OWN HARDWARE

4 INSTALLING AND RECOVERING HIGH AVAILABILITY (HA) QRADAR SIEM APPLIANCES

5 INSTALLING AND RECOVERING HIGH AVAILABILITY (HA) SOFTWARE

6 RE-INSTALLING QRADAR SIEM FROM THE RECOVERY PARTITION

7 INSTALLING A VIRTUAL APPLIANCE

8 CHANGING NETWORK SETTINGS

A NOTICES AND TRADEMARKS

INDEX

ABOUT THIS GUIDE

The *IBM Security QRadar SIEM Installation Guide* provides you with information on installing QRadar SIEM 7.1 (MR1). QRadar SIEM appliances are pre-installed with software and a Red Hat Enterprise Linux version 6.3 operating system; however, you can install QRadar SIEM software on your own hardware. This guide assumes a working knowledge of networking and Linux systems.

Intended Audience

This guide is intended for network administrators responsible to installing and configuring QRadar SIEM systems in your network.

Documentation Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

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)

1 PREPARING FOR YOUR INSTALLATION

This section provides information on preparing your QRadar SIEM installation. To ensure a successful QRadar SIEM deployment, adhere to the recommendations in this document.

This section includes the following topics:

- **QRadar SIEM Deployments**
- **Additional Hardware Requirements**
- **Additional Software Requirements**
- **Supported Browsers**
- **Identifying Network Settings**
- **Preparing Your Network Hierarchy**
- **Identifying Security Monitoring Log Sources**
- **Preparing For HA**
- **Using the Installation Wizard**
- **Accessing the QRadar SIEM User Interface**

QRadar SIEM Deployments

Your IBM Security QRadar SIEM deployment can consist of QRadar SIEM installed on one or multiple systems. You can use the QRadar SIEM three-tier architecture 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.

You can install QRadar SIEM on QRadar appliances or QRadar SIEM software installed on your own hardware. A QRadar appliance includes QRadar SIEM software and a Red Hat Enterprise Linux operating system. For further information about QRadar appliances, see the *Hardware Installation Guide*.

QRadar SIEM components that can exist in your deployment include:

- **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 user interface for QRadar SIEM. The Console provides real time views, reports, alerts, and in-depth flow views of network traffic and security threats. Using the Console, you can also manage distributed QRadar SIEM deployments.

  You can access the Console from a standard web browser. When you access the system, a prompt is displayed for a username and password, which you configure during the installation process. You must also have Java™ installed on your desktop system. For information about software requirements, see **Additional Software Requirements**.
- **Event Collector** - The Event Collector gathers events from local and remote device sources. The Event Collector normalizes events, and then sends the information to the Event Processor. Before sending information to the Event Processor, the Event Collector bundles identical events to conserve system usage. During this process, the Magistrate examines the event from the device and maps the event to a QRadar Identifier (QID), and then creates the bundles.
- **Event Processor** - Processes events collected from one or more Event Collector. When received, 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. Rules are applied to the events that allow the Event Processor to process events according to the configured rules. When complete, the Event Processor sends the events to the Magistrate.
- **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 the event against the defined custom rules to create an offense. If there is no match to a custom rule, the Magistrate uses default rules to process the event. An offense is an event that has been processed through QRadar SIEM 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.

NOTE

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

Additional Hardware Requirements

Before installing your QRadar SIEM systems, make sure you have access to the additional hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS)

NOTE

To make sure that your QRadar SIEM data is preserved during a power failure, we recommend that all QRadar SIEM appliances or systems running QRadar SIEM software that store data, such as Consoles, Event Processors, or QRadar QFlow Collectors are equipped with a Uninterrupted Power Supply (UPS).

Additional Software Requirements

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

- Java^{TM} Runtime Environment (JRE) installed on the desktop system you plan to use to view QRadar SIEM. You can download Java 1.6.0_u24 at the following website: *http://java.com/*.
- Adobe Flash 10.x installed on the desktop you plan to use to access the QRadar SIEM Console.

NOTE

Make sure that you install JRE on your desktop system, not the QRadar SIEM appliance.

Supported Browsers

You can access the Console from a standard web browser. When you access the system, a prompt is displayed asking for a user name and a password, which must be configured in advance by the QRadar 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 testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating 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 enable Compatibility View for Microsoft Internet Explorer 8.0 and 9.0:

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.**

Identifying Network Settings

Before you install QRadar SIEM, you must gather 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 (optional) address
- Public IP address for networks using Network Address Translation (NAT)
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

If you have already installed QRadar SIEM 7.1 (MR1) and are recovering a failed primary HA host, you must also gather the following information from the QRadar SIEM user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the *IBM Security QRadar SIEM Administration Guide.*

Preparing Your Network Hierarchy

QRadar SIEM uses the network hierarchy to understand your network traffic and provide you with the ability to view network activity for your entire deployment. QRadar SIEM supports any network hierarchy that can be defined by a range of IP addresses. You can create your network hierarchy based on many different variables, including geographical or business units. For example, your network hierarchy might include corporate IP address ranges (internal or external), physical departments or areas, mails servers, and web servers.

After you define the QRadar SIEM components that you want to add to your network hierarchy and install QRadar SIEM, you can then configure the network hierarchy using the QRadar SIEM Console.

▶ For each QRadar SIEM component that you want to add to your network hierarchy, record each network component (object) in your network map.

At a minimum, we recommend that you define objects in the network hierarchy for:

- Internal and external Demilitarized zones (DMZs)
- Virtual Private Networks (VPNs)
- All internal IP address spaces (for example, 10.0.0.0/8)
- Proxy servers
- (NAT) IP address range
- Server Network subnets
- Voice over IP (VoIP) subnets

For more information, see the *IBM Security QRadar SIEM Administration Guide - Setting Up IBM Security QRadar SIEM, Creating Your Network Hierarchy*.

Identifying Security Monitoring Log Sources

QRadar SIEM collects and correlates events received from log sources which are external devices such as:

- Security equipment, such as firewalls, VPNs, and Intrusion Detection Systems (IDSs)
- Host or application security logs such as window logs

Device Support Modules (DSMs) and QRadar QFlow Collectors allow you to integrate QRadar SIEM data from these log sources.

QRadar SIEM automatically discovers log sources that send syslog messages to an Event Collector. Automatically discovered log sources are displayed in the Log Sources window within the **Admin** tab. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

You must add non-syslog based log sources to your deployment manually. For each non-syslog log source that you want to add to your deployment, record the following information:

- **Log Source Type** - Specifies the type of log source, such as firewall, router, or VPN log sources.
- **QTY** - Specifies how many devices you have of this log source type.
- **Product Name/Version** - Specifies the log source product name and version number.
- **Link Speed & Type** - Specifies the maximum network link speed (in Kbps) for firewall, router, and VPN log sources. For the type, record the primary application of the host system, for example, email, anti-virus, domain controller, or a workstation.
- **Msg Level** - Specifies the message level that you want to log for this log source type. For example, critical, informational, or debug.
- **Avg Log Rate (Event/Sec)** - Specifies the average event rate per second.
- **No. of Users** - Specifies the maximum number of hosts or users using or being served by this log source.
- **Network Location** - Specifies whether this log source is located on the DMZ, Internet, Intranet, or Extranet.
- **Geographic Location** - Specifies if the log sources are located on the same Local Area Network (LAN) as QRadar SIEM or if they are sending logs over the Wide Area Network (WAN).
- **Credibility** - Specifies the integrity of an event or offense as determined by the credibility rating from log sources. Credibility increases as multiple sources report the same event.

For more information, see the *Managing Log Sources Guide*.

Preparing For HA

Before deploying HA in your environment, ensure your HA hosts adhere to the following requirements:

- The secondary host must have a valid HA activation key.
- The secondary host must have the same QRadar SIEM software version and patch level installed as the primary host in the HA cluster.
- The secondary host’s memory must be equal to or greater than the primary host’s memory.
- The secondary host must be located on the same subnet as the primary host.
- The secondary host’s /store partition must be larger than the /store partition on the primary host.
- If you plan to enable disk synchronization, we recommend that there is at least a 1 GB connection between the primary host and secondary host.

- If you plan for your HA hosts to share external storage, we recommend that there is at least a 1 GB connection between each HA host and your external storage solution.

Using the Installation Wizard

The following table provides instruction on how to use and navigate the installation wizard:

Table 1-3 Installation Wizard Actions

If you want to	Perform this action
Move to another option on a page	Press the Up or Down arrows to move the cursor through configurable options on the installation wizard page.
Select an option from a list	Press the Spacebar to select your chosen option on a list. When you select an option, an X is displayed in the parentheses next to the option.
Select a navigation option	Press Tab to move the cursor from the configurable options to the **Next**, **Back**, and **Finish** options.
Select a navigation option	Press Enter on the keyboard.

Accessing the QRadar SIEM User Interface

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

To access the QRadar SIEM user interface:

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>**

Where `<root password>` is the password assigned to QRadar SIEM during the installation process.

NOTE

If you are using Mozilla Firefox, you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla documentation. If you are using Internet Explorer, a website security certificate message is displayed. You must select the Continue to this website option to log in to QRadar SIEM.

Step 3 Click **Login 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*.

2 INSTALLING QRADAR SIEM APPLIANCES

A QRadar SIEM appliance includes QRadar SIEM software and a Red Hat Enterprise Linux operating system. For more information about appliances, see the *Hardware Installation Guide*.

Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

This section includes the following topics:

- **Installing a QRadar SIEM Appliance (Consoles)**
- **Installing a QRadar QFlow Appliance (Non-Consoles)**

Installing a QRadar SIEM Appliance (Consoles)

To install a QRadar SIEM appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document.

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

The activation key window is displayed. 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.

g Type your activation key and press Enter.

NOTE

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

Step 2 Select **normal** for the type of setup. Select **Next** and press Enter.

Step 3 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 4 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 **Step 5**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 6**.

Step 5 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 9**.

Step 6 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 7 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 8 Select your time zone region. Select **Next** and press Enter.

Step 9 Select an internet protocol version. Select **Next** and press Enter.

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

Step 10 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 11 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 14**.

- If you are using IPv6 as your Internet protocol, go to **Step 12**.

Step 12 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 14**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 13**.

Step 13 To 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 15**

Step 14 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. 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.
- **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 15 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.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

Step 16 Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

Installing a QRadar QFlow Appliance (Non-Consoles)

To set up your QRadar QFlow appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

  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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

f Type your activation key and press Enter.

NOTE

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

Step 2 Select **normal** for your type of setup. Select **Next** and press Enter.

Step 3 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 4 Select your time zone region. Select **Next** and press Enter.

Step 5 Select an internet protocol version. Select **Next** and press Enter.

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

Step 6 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 7 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 10**.
- If you are using IPv6 as your Internet protocol, go to **Step 8**.

Step 8 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 10**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 9**.

Step 9 To 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 10 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. 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.

- **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 11 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.

c Select **Finish** and press Enter.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

d Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

3 INSTALLING QRADAR SIEM SOFTWARE ON YOUR OWN HARDWARE

This section provides information on installing IBM Security QRadar SIEM software on your own hardware using the Red Hat Enterprise Linux 6.3 operating system. Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

This section includes the following topics:

Before You Begin

QRadar SIEM supports the 64-bit versions of the Red Hat Enterprise Linux 6.3 operating system. Before you install the Red Hat Enterprise Linux 6.3 operating system, note the following:

- When installing the Red Hat Enterprise Linux operating system, you must use the **Base** install option and set the SELinux option to **Disabled**. If you do not adhere to this recommendation, your installation will fail.

NOTE

To access the **Base** install option, select the **Customize Software Packages to be Installed** option and clear all the options in each category except **BASE** in the Base System category.

- QRadar SIEM does not support KickStart disks. Using 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, make sure the primary drive is at least 256 GB. For QRadar QFlow Collector, make sure the primary drive is at least 36 GB. The Console must have at least 8 GB of RAM. We strongly recommend that your Console has at least 24 GB of RAM if you plan to enable payload indexing. We require that you upgrade your system memory before installing QRadar SIEM on your system.
- The firewall configuration must allow WWW (http, https) and SSH traffic. Prior to configuring the firewall, disable the SELinux option. During the QRadar SIEM

installation, a default firewall template is installed, which you can update using the System Setup window.

Installing QRadar SIEM Console Software On Your Own Hardware

To install QRadar SIEM Console software on your own hardware using the Red Hat Enterprise Linux 6.3 operating system:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

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

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, then you are required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 Select **normal** for your type of setup. Select **Next**.

Step 11 To specify that you want to install a Console system, select **This system is a console**. Select **Next**.

The Tuning Template window is displayed.

Step 12 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 13 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 **Step 14**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 15**.

Step 14 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 18**.

Step 15 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 16 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 17 Select your time zone region. Select **Next** and press Enter.

Step 18 Select an internet protocol version. Select **Next** and press Enter.

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

Step 19 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 20 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 23**.
- If you are using IPv6 as your Internet protocol, go to **Step 21**.

Step 21 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 23**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 22**.

Step 22 To 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 24**.

Step 23 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. 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.
- **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 24 Configure the QRadar SIEM root password:

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

The Confirm New Root Password window is displayed.

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

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

Step 25 Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

Installing QRadar SIEM Non-Console Software On Your Own Hardware

To install QRadar SIEM non-Console software on your own hardware using the Red Hat Enterprise Linux 6.3 operating system:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

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

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, you will be required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 Select **normal** for your type of setup. Select **Next**.

The Time Zone Continent window is displayed.

Step 11 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 12 Select your time zone region. Select **Next** and press Enter.

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

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

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

Step 15 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 18**.
- If you are using 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 To 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. 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.

- **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 Confirm New Root Password window is displayed.

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

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

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

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

Installing and Configuring the Red Hat Enterprise Linux Operating System

To install and configure the Red Hat Enterprise Linux 6.3 operating system:

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 To load the boot menu, press the F11 key or the Escape key on your keyboard.

e Select the USB drive or DVD drive as the boot option.

CAUTION

If you are installing 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.

The Welcome page of the installation wizard is displayed.

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

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 during 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 **Manual** 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**.

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:

CAUTION

Your upgrade will fail if you reformat any of the following partitions or their sub-partitions: /store, /store/tmp, /store/ariel, /store/persistent data.

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

If you want to delete and recreate these partitions instead of editing them, use the following table as a guide:

Table 1-1 Partitioning 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 during the creation of software RAID partitions, contact Customer Support.

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.

Step 16 Click **Next**.

No changes are required on this page.

Step 17 Click **Next**.

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

The operating system installation proceeds.

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

4 Installing and Recovering High Availability (HA) QRadar SIEM Appliances

This section provides information on installing or recovering your IBM Security QRadar SIEM High Availability (HA) appliances. Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

This section includes the following topics:

- **Before You Begin**
- **Installing a Secondary HA QRadar SIEM Appliance**
- **Installing a Secondary HA QRadar QFlow Appliance**
- **Recovering a Failed Primary HA QRadar SIEM Appliance**
- **Recovering a Failed Primary HA QRadar QFlow Appliance**
- **Recovering a Failed Secondary HA Host to the QRadar SIEM 7.1 (MR1)**
- **Recovering a QRadar SIEM Secondary HA Host to a Previous Version or Factory Default**

Before You Begin

Before deploying HA in your environment, ensure your HA hosts adhere to the following requirements:

- The secondary host must have a valid High Availability (HA) activation key.
- The secondary host must have the same QRadar SIEM software version installed as the primary host in the HA cluster.
- The secondary host's memory must be equal to or greater than the primary host's memory.
- The secondary host must be located on the same subnet as the primary host.
- The secondary host's /store partition must be larger than the /store partition on the primary host.
- If you plan to enable disk synchronization, we recommend that there is at least a 1 GB connection between the primary host and secondary host.
- If you plan for your HA hosts to share external storage, we recommend that there is at least a 1 GB connection between each HA host and your external storage solution.

Installing a Secondary HA QRadar SIEM Appliance

To install your secondary HA QRadar SIEM appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

f Type your activation key and press Enter.

NOTE

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

Step 2 To specify your secondary device type, select **This system is a stand-by for a console**. Select **Next** and press Enter.

Step 3 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 **Step 4**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 5**.

Step 4 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 8**.

Step 5 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 6 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 7 Select your time zone region. Select **Next** and press Enter.

Step 8 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

Step 9 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 10 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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

- **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. 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.

- **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.

NOTE

If you are changing network settings using qchange_netsetup, select **Finish** and press Enter. See **Changing Network Settings**.

Step 11 To configure the QRadar SIEM root password:

a Type your password.

The password must meet the following criteria:

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

b Select **Next** and press Enter.

The Confirm New Root Password window is displayed.

c Retype your new password to confirm.

d Select **Finish** and press Enter.

A series of messages is displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

e Press Enter to select **OK**.

Step 12 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 13 Configure your HA cluster. For more information on configuring your HA cluster, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

Installing a Secondary HA QRadar QFlow Appliance

To install your secondary HA QRadar QFlow appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

f Type your activation key and press Enter.

NOTE

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

Step 2 To specify your secondary device type, select **This system is a stand-by for a non-console**. Select **Next** and press Enter.

Step 3 Select the time zone continent. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 4 Select your time zone region. Select **Next** and press Enter.

Step 5 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

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

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

Step 6 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 7 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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 8 To 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** option and press Enter.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 9 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 10 Configure your HA cluster. For more information on configuring your HA cluster, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

Recovering a Failed Primary HA QRadar SIEM Appliance

Before you recover a failed primary HA appliance, you must gather the following information from the QRadar SIEM user interface:

- Cluster Virtual IP Address
- Primary IP Address

You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

CAUTION

If your HA cluster uses shared storage, you must manually configure iSCSI. For more information about configuring iSCSI, see the Configuring iSCSI Technical Note.

To recover a failed primary HA QRadar SIEM appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

f Type your activation key and press Enter.

NOTE

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

Step 2 To specify your type of setup, select **HA Recovery Setup**. Select **Next** and press Enter.

Step 3 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 **Step 4**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 5**.

Step 4 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 8**.

Step 5 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 6 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 7 Select your time zone region. Select **Next** and press Enter.

Step 8 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

Step 9 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 10 Type the Cluster Virtual IP address. Select **Next** and press Enter.

The Cluster Virtual IP address is the original IP address of the primary HA system. You can find this IP address in the System and License Management window by pointing your mouse over the row for the HA cluster.

Step 11 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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see *the IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 12 To 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.

A series of messages is displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 13 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 14 Using the user interface, restore the failed primary HA system. For more information on restoring a failed primary HA system, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

Recovering a Failed Primary HA QRadar QFlow Appliance

Before you recover a failed primary HA QRadar QFlow appliance, you must gather the following information from the QRadar SIEM user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

CAUTION

If your HA cluster uses shared storage, you must manually configure iSCSI. For more information about configuring iSCSI, see the Configuring iSCSI Technical Note.

To recover a failed primary HA QRadar QFlow appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

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

b Choose one of the following options:

- Connect a laptop to the serial port on the rear of the appliance.

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).

- Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

c Power on the system and log in:

Username: **root**

NOTE

The username is case sensitive.

d Press Enter.

The End User License Agreement (EULA) is displayed.

e Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

f Type your activation key and press Enter.

NOTE

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

Step 2 To specify your type of setup, select **HA Recovery Setup**. Select **Next** and press Enter.

Step 3 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 4 Select your time zone region. Select **Next** and press Enter.

Step 5 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

Step 6 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 7 Type the Cluster Virtual IP address. Select **Next** and press Enter.

The Cluster Virtual IP address is the original IP address of the primary HA system. You can find this IP address in the System and License Management window by pointing your mouse over the row for the HA cluster.

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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 9 To 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.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 10 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 11 Using the user interface, restore the failed primary HA system. For more information on restoring a failed primary HA system, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

Recovering a Failed Secondary HA Host to the QRadar SIEM 7.1 (MR1)

When recovering a failed secondary HA host that used a previous QRadar SIEM version, you can install QRadar SIEM 7.1 (MR1) from an updated recovery partition.

To recover a failed secondary HA host from the recovery partition:

Step 1 Using SSH, log in to the secondary HA host as the root user.

Username: root

Password: <password>

Step 2 Obtain the QRadar SIEM software from the Qmmunity website.

Step 3 To copy the QRadar SIEM 7.1 (MR1) ISO to the secondary HA host, type the following command:

```
scp <iso file name> root@<ip_address>:/root
```

CAUTION

If you are installing QRadar SIEM 7.0 and above, Step 4 and Step 5 are not required because the recovery script is placed in /opt/qradar/bin during the installation.

Step 4 To mount the ISO, type the following command:

```
mount -o loop <iso_file_name> /media/cdrom/
```

Step 5 To copy the recover script into the root directory, type the following command:

```
cp /media/cdrom/post/recovery.py /root
```

Step 6 To unmount the ISO, type the following command:

```
umount /media/cdrom/
```

Step 7 If the host is a non-Console, stop the IPTables service to allow SCP. Type the following command: `service iptables stop`.

Step 8 To start the extracted recovery script, type the following command:

```
./recovery.py -r --default --reboot <iso_file_name>
```

Step 9 When prompted, press Enter to reboot the appliance.

Step 10 When prompted, type `flatten` and press Enter.

The installer repartitions and reformats the hard disk, installs the Operating System, and then re-installs QRadar SIEM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When this process is complete, the normal installation process proceeds.

For more information on installing your secondary HA host, choose one of the following:

- **Installing a Secondary HA QRadar SIEM Appliance**
- **Installing a Secondary HA QRadar QFlow Appliance**

Step 11 When the installation completes, type **`SETUP`** and log in to the system as the root user.

Recovering a QRadar SIEM Secondary HA Host to a Previous Version or Factory Default

Using this procedure, you can recover a failed QRadar SIEM secondary HA host that does not include a recovery partition or a USB port to a previous version or restore the system to factory defaults. When you recover the failed secondary HA host, all data removed and the factory default configuration is restored on the host.

To restore a secondary HA host to a previous version or factory default:

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

Step 2 Using SCP, copy the recovery.py script from the Console to the failed secondary HA host.

By default, th recovery.py script is downloaded to the /root directory if you do not specify a location.

Step 3 Go to the Qmmunity website to download the ISO image for the QRadar SIEM version you want to restore.

Step 4 Using SCP, copy the ISO to the target QRadar SIEM host.

Step 5 Using SSH, log in to the secondary HA host.

Step 6 Type the following commands:

```
Chmod 755 recovery.py
./recovery.py -r --default --reboot <iso_file_name>
```

Step 7 Press Enter when prompted to reboot the system.

The system restarts.

Step 8 When prompted, type **`flatten`** and press Enter.

The installer repartitions and reformats the hard disk, installs the Operating System, and then installs QRadar SIEM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When this process is complete, the normal installation process proceeds.

For more information on installing your secondary HA host, choose one of the following:

- **Installing a Secondary HA QRadar SIEM Appliance**
- **Installing a Secondary HA QRadar QFlow Appliance**

5 INSTALLING AND RECOVERING HIGH AVAILABILITY (HA) SOFTWARE

This section provides information on installing or recovering your QRadar SIEM High Availability (HA) systems. Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

This section includes the following topics:

- **Before You Begin**
- **Installing QRadar SIEM Console Software On Your Secondary HA System**
- **Installing QRadar SIEM Non-Console Software On Your Secondary HA System**
- **Recovering QRadar SIEM Console Software on Your Failed Primary HA Host**
- **Recovering QRadar SIEM Non-Console Software on Your Failed Primary HA Host**
- **Recovering a Failed Secondary HA Host to the QRadar SIEM 7.1 (MR1)**
- **Recovering a QRadar SIEM Secondary HA Host to a Previous Version or Factory Default**

Before You Begin

Before deploying HA in your environment, ensure your HA hosts adhere to the following requirements:

- The secondary host must have a valid High Availability (HA) activation key.
- The secondary host must have the same QRadar SIEM software version installed as the primary host in the HA cluster.
- The secondary host's memory must be equal to or greater than the primary host's memory.
- The secondary host must be located on the same subnet as the primary host.
- The secondary host's /store partition must be larger than the /store partition on the primary host.
- If you plan to enable disk synchronization, we recommend that there is at least a 1 GB connection between the primary host and secondary host.
- If you plan for your HA hosts to share external storage, we recommend that there is at least a 1 GB connection between each HA host and your external storage solution.

Installing QRadar SIEM Console Software On Your Secondary HA System

To install QRadar SIEM Console software on your secondary HA system:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

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

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, you will be required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 To specify your secondary device type, select **This system is a stand-by for a console**. Select **Next** and press Enter.

Step 11 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 Step 12.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to Step 13.

Step 12 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to Step 16.

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

The Time Zone Continent window is displayed.

Step 14 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 15 Select your time zone region. Select **Next** and press Enter.

Step 16 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

Step 17 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

- **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. 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.
- **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.

NOTE

If you are changing network settings using qchange_netsetup, select **Finish** and press Enter. See **Changing Network Settings**.

Step 19 To configure the QRadar SIEM root password:

a Type your password.

The password must meet the following criteria:

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

b Select **Next** and press Enter.

The Confirm New Root Password window is displayed.

c Retype your new password to confirm.

d Select **Finish** and press Enter.

A series of messages is displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

e Press Enter to select **OK**.

Step 20 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 21 Configure your HA cluster. For more information on configuring your HA cluster, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

Installing QRadar SIEM Non-Console Software On Your Secondary HA System

To install QRadar SIEM non-Console software on your secondary HA system:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

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

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, you will be required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 To specify your secondary device type, select **This system is a stand-by for a non-console**. Select **Next** and press Enter.

Step 11 Select the time zone continent. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 12 Select your time zone region. Select **Next** and press Enter.

Step 13 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

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

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 To 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** option and press Enter.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 17 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 18 Configure your HA cluster. For more information on configuring your HA cluster, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability.*

Recovering QRadar SIEM Console Software on Your Failed Primary HA Host

Before you recover a failed primary HA host, you must gather the following information from the QRadar SIEM user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

To recover a failed primary HA Console host on your own hardware:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

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

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, you will be required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 To specify your type of setup, select **HA Recovery Setup**. Select **Next** and press Enter.

Step 11 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 **Step 12**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 13**.

Step 12 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 16**.

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

The Time Zone Continent window is displayed.

Step 14 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 15 Select your time zone region. Select **Next** and press Enter.

Step 16 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

Step 17 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 18 Type the Cluster Virtual IP address. Select **Next** and press Enter.

The Cluster Virtual IP address is the original IP address of the primary HA system. You can find this IP address in the System and License Management window by pointing your mouse over the row for the HA cluster.

Step 19 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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see *the IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 20 To 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.

A series of messages is displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 21 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 22 Using the user interface, restore the failed primary HA system. For more information on restoring a failed primary HA system, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

Recovering QRadar SIEM Non-Console Software on Your Failed Primary HA Host

Before you recover a failed primary HA host, you must gather the following information from the QRadar SIEM user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

To recover a failed primary HA non-console host on your own hardware:

Step 1 Install the necessary hardware.

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

For instructions on how to install and configure the Red Hat Enterprise Linux 6.3 operating system, see **Installing and Configuring the Red Hat Enterprise Linux Operating System**.

Step 3 Log in as root.

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

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar SIEM software from the Qmmunity website.

Step 6 To mount the QRadar SIEM 7.1 (MR1) ISO, type:

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

Step 7 To begin the installation, type:

/media/cdrom/setup

NOTE

QRadar SIEM verifies the integrity of the media before installation by checking the MD5 sum. If you receive a warning message that the MD5 checksum failed, you will be required to re-download or re-burn QRadar SIEM. For further assistance, contact Customer Support.

The End User License Agreement (EULA) is displayed.

Step 8 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. 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.

Step 9 Type your activation key and press Enter.

NOTE

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

Step 10 To specify your type of setup, select **HA Recovery Setup**. Select **Next** and press Enter.

Step 11 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 12 Select your time zone region. Select **Next** and press Enter.

Step 13 Select **IPv4** for your internet protocol version. Select **Next** and press Enter.

NOTE

IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error message is displayed. In this case, select **Back** and then select **IPv4**. You can then proceed to next step in your installation.

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

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

Step 15 Type the Cluster Virtual IP address. Select **Next** and press Enter.

The Cluster Virtual IP address is the original IP address of the primary HA system. You can find this IP address in the System and License Management window by pointing your mouse over the row for the HA cluster.

Step 16 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.

NOTE

If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

- **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. 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.
- **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 17 To 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.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 18 Log in to the QRadar SIEM user interface. See **Accessing the QRadar SIEM User Interface**.

Step 19 Using the user interface, restore the failed primary HA system. For more information on restoring a failed primary HA system, see the *IBM Security QRadar SIEM Administration Guide - Managing High Availability*.

Recovering a Failed Secondary HA Host to the QRadar SIEM 7.1 (MR1)

When recovering a failed secondary HA host that used a previous QRadar SIEM version, you can install QRadar SIEM 7.1 (MR1) from an updated recovery partition.

To recover a failed secondary HA host from the recovery partition:

Step 1 Using SSH, log in to the secondary HA host as the root user.

Username: root

Password: <password>

Step 2 Obtain the QRadar SIEM software from the Qmmunity website.

Step 3 To copy the QRadar SIEM 7.1 (MR1) ISO to the secondary HA host, type the following command:

```
scp <iso file name> root@<ip_address>:/root
```

CAUTION

If you are installing QRadar SIEM 7.0 and above, **Step 4** *through* **Step 5** *are not required because the recovery script is placed in /opt/qradar/bin during the installation.*

Step 4 To mount the ISO, type the following command:

```
mount -o loop <iso_file_name> /media/cdrom/
```

Step 5 To copy the recover script into the root directory, type the following command:

```
cp /media/cdrom/post/recovery.py /root
```

Step 6 To unmount the ISO, type the following command:

```
umount /media/cdrom/
```

Step 7 If the host is a non-Console, stop the IPTables service to allow SCP. Type the following command: `service tables stop`.

Step 8 To start the extracted recovery script, type the following command:

```
./recovery.py -r --default --reboot <iso_file_name>
```

Step 9 When prompted, press Enter to reboot the appliance.

Step 10 When prompted, type `flatten` and press Enter.

The installer repartitions and reformats the hard disk, installs the Operating System, and then re-installs QRadar SIEM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When this process is complete, the normal installation process proceeds.

For more information on installing your secondary HA host, choose one of the following:

- **Installing QRadar SIEM Console Software On Your Secondary HA System**
- **Installing QRadar SIEM Non-Console Software On Your Secondary HA System**

Step 11 When the installation completes, type **`SETUP`** and log in to the system as the root user.

Recovering a QRadar SIEM Secondary HA Host to a Previous Version or Factory Default

Using this procedure, you can recover a failed QRadar SIEM secondary HA host that does not include a recovery partition or a USB port to a previous version or restore the system to factory defaults. When you recover the failed secondary HA host, all data removed and the factory default configuration is restored on the host.

To restore a secondary HA host to a previous version or factory default:

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

Step 2 Using SCP, copy the recovery.py script from the Console to the failed secondary HA host.

By default, th recovery.py script is downloaded to the /root directory if you do not specify a location.

Step 3 Go to the Qmmunity website to download the ISO image for the QRadar SIEM version you want to restore.

Step 4 Using SCP, copy the ISO to the target QRadar SIEM host.

Step 5 Using SSH, log in to the secondary HA host.

Step 6 Type the following commands:

```
Chmod 755 recovery.py
./recovery.py -r --default --reboot <iso_file_name>
```

Step 7 Press Enter when prompted to reboot the system.

The system restarts.

Step 8 When prompted, type **`flatten`** and press Enter.

The installer repartitions and reformats the hard disk, installs the Operating System, and then installs QRadar SIEM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When this process is complete, the normal installation process proceeds.

For more information on installing your secondary HA host, choose one of the following:

- **Installing QRadar SIEM Console Software On Your Secondary HA System**
- **Installing QRadar SIEM Non-Console Software On Your Secondary HA System**

6 RE-INSTALLING QRADAR SIEM FROM THE RECOVERY PARTITION

This section provides information about re-installing IBM Security QRadar SIEM software from the recovery partition. When you re-install QRadar SIEM, your system is restored back to factory default configuration, meaning that your current configuration and data files are overwritten. Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

NOTE

This section applies to new QRadar SIEM 7.1 (MR1) installations or upgrades from new QRadar SIEM 7.0 installations on QRadar SIEM appliances.

When you install QRadar SIEM 7.1 (MR1), 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.

NOTE

Any software upgrades you perform after you install QRadar SIEM 7.1 (MR1) replaces the ISO file with the newer version.

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 maintaining your configuration and data files. 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.

This section includes the following topics:

- **Preparing for Re-installation from a Recovery Partition**
- **Re-installing a QRadar SIEM Appliance**
- **Re-installing a QRadar QFlow Collector Appliance**

Preparing for Re-installation from a Recovery Partition

To prepare for re-installation:

Step 1 Reboot your QRadar SIEM appliance.

A menu is displayed with the following options:

- **Normal System** - Starts QRadar SIEM as normal.
- **Factory re-install** - Runs the installer.

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

The installer runs and detects that there is already an installation present.

Step 3 Type `flatten` to continue.

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, depending on your system. When the process is complete, a confirmation is displayed:

Step 4 Type `SETUP`.

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

Username: root

Password: <password>

The End User License Agreement (EULA) is displayed.

Step 6 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM

You can find the key:

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

NOTE

If you do not have your activation key, contact the Welcome Center at welcomecenter@q1labs.com with the serial number of the QRadar SIEM appliance. Software activation keys do not require serial numbers.

Step 7 Type your activation key and press Enter.

NOTE

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

If you are setting up a QRadar SIEM appliance, such as a QRadar SIEM 2100, the Tuning Template window is displayed. Go to **Re-installing a QRadar SIEM Appliance**.

If you are setting up a QRadar QFlow Collector appliance, such as a QRadar QFlow 1201, the Time Zone Continent window is displayed. Go to **Re-installing a QRadar QFlow Collector Appliance**.

Re-installing a QRadar SIEM Appliance

To re-install a QRadar SIEM appliance:

Step 1 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 2 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 **Step 3**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 4**.

Step 3 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 7**.

Step 4 To specify a time server, in the **Time server** field, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 5 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 6 Select your time zone region. Select **Next** and press Enter.

Step 7 Select an internet protocol version. Select **Next** and press Enter.

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

Step 8 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 9 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 12**.
- If you are using IPv6 as your Internet protocol, go to **Step 10**.

Step 10 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 12**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 11**.

Step 11 To 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 13**.

Step 12 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. 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.
- **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 13 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.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

Step 14 Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

Re-installing a QRadar QFlow Collector Appliance

To re-install a QRadar QFlow Collector appliance:

Step 1 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 2 Select your time zone region. Select **Next** and press Enter.

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

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

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

Step 5 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 8**.
- If you are using 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 To 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. 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.

- **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.

NOTE

If you are changing network settings using qchange_netsetup, select **Finish** and press Enter. See **Changing Network Settings**.

Step 9 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.

c Select **Finish** and press Enter.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

d Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

7 INSTALLING A VIRTUAL APPLIANCE

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

This section includes the following topics:

- **QRadar SIEM Virtual Appliances**
- **Before You Begin**
- **Preparing Your Virtual Machine for QRadar SIEM Installation**
- **Installing QRadar SIEM Software on Your Virtual Machine**

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

QRadar SIEM Virtual Appliances

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 expand the capacity of the QRadar SIEM 3190 beyond license-based upgrade options by adding one or more of the following virtual appliances:

- 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.

Before You Begin

Before you install your virtual appliance, note the following:

- Virtual appliances require VMware ESXi 4.1. You must have a VMware client installed on your desktop. VMware server applications are bundled with client software. For example, ESXi 4.1 is bundled with VMware vSphere client 4.1. 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 36 GB of free disk space.

Preparing Your Virtual Machine for QRadar SIEM Installation

This section includes the following topics:

- **Creating your Virtual Machine**
- **Installing the QRadar SIEM ISO on the Virtual Machine**

Creating your Virtual Machine

To create your virtual machine:

Step 1 Access your vSphere Client.

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

The Create New Virtual Machine window is displayed.

Step 3 In the Configuration pane, 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 Specify the guest 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 From the **Number of virtual processors** list box, select the number of processors that you want for the virtual machine and click **Next**. You must select a minimum of 2 processors.

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 **Allocate and commit space on demand (Thin provisioning)** check box.

c Click **Next**.

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

Step 14 Click **Next**.

The Ready to Complete page is displayed. Review the settings for your new virtual machine and edit the settings if required.

Step 15 Click **Finish**.

Your virtual machine is ready for optimal performance when running your QRadar SIEM virtual appliance.

Installing the QRadar SIEM ISO on the Virtual Machine

To install QRadar SIEM software on a virtual appliance:

Step 1 Obtain the QRadar SIEM software from the Qmmunity website.

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**.

The Virtual Machine Properties window is displayed.

Step 5 In the left pane, 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**.

The Browse Datastores window is displayed.

Step 8 Locate and select the ISO file and click **Open**.

Step 9 Click **OK**.

The virtual machine is now ready to power up and install QRadar SIEM. For more information, see **Installing QRadar SIEM Software on Your Virtual Machine**.

Installing QRadar SIEM Software on Your Virtual Machine

Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

To install QRadar SIEM software on your virtual machine:

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.

The End User License Agreement (EULA) is displayed.

Step 5 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document.

Step 6 Type **yes** to accept the agreement, and then press Enter.

The activation key window is displayed. The activation key is a 24-digit, four-part, alphanumeric string that you receive from IBM

Step 7 Type your activation key and press Enter.

NOTE

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

Step 8 Select **normal** for your type of setup. Select **Next** and press Enter.

Step 9 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.

NOTE

If you select **Yes** to indicate that your system is a Console, an error message is displayed if your system has less than 8 GB of RAM. We require that you upgrade the memory on your system before installing QRadar SIEM on your system.

d Select **Next** and press Enter.

Step 10 Select the **Enterprise** tuning template. Select **Next** and press Enter.

Step 11 Select method that you want to use to set the date and time:

- **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 **Step 12**.
- **Server** - Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed. Go to **Step 13**.

Step 12 To manually enter the time and date, type the current date and time. Select **Next** and press Enter. Go to **Step 14**.

Step 13 To specify a time server, type the time server name or IP address. Select **Next** and press Enter.

The Time Zone Continent window is displayed.

Step 14 Select your time zone continent or area. Select **Next** and press Enter.

The Time Zone Region window is displayed.

Step 15 Select your time zone region. Select **Next** and press Enter.

Step 16 Select an internet protocol version. Select **Next** and press Enter.

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

Step 17 Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

Step 18 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 21**.
- If you are using IPv6 as your Internet protocol, go to **Step 19**.

Step 19 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 21**.

b To manually configure for IPv6, select **No** and press Enter. Go to **Step 20**.

Step 20 To enter network information to use for IPv6, type the values for the **Hostname** and **Email server**. Select **Next** and press Enter.

Step 21 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. 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.
- **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.

NOTE

If you are changing network settings using the qchange_netsetup utility, select **Finish** and press Enter. See **Changing Network Settings**.

Step 22 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.

A series of messages are displayed as QRadar SIEM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

You are now ready to access QRadar SIEM. For more information on accessing QRadar SIEM, see **Accessing the QRadar SIEM User Interface**.

Adding Your Virtual Appliance to Your Deployment

To add your virtual appliance to your deployment:

Step 1 Log in to the QRadar SIEM Console.

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

The Event View page is displayed.

Step 2 In the Event Components pane, select the virtual appliance component that you want to add.

The Adding a New Component wizard is displayed.

Step 3 Type a unique name for the virtual appliance. The name can be up to 20 characters in length and may include underscores or hyphens. Click **Next**.

The Assign Component page is displayed.

Step 4 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 5 Click **Finish**.

Step 6 From the deployment editor menu, select **File > Save to staging**.

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

Step 7 On the **Admin** tab menu, click **Deploy Changes**.

8 CHANGING NETWORK SETTINGS

This section includes the following topics:

- **Changing Network Settings in an All-in-One Console**
- **Changing the Network Settings of a Console in a Multi-System Deployment**
- **Changing the Network Settings of a Non-Console in a Multi-System Deployment**
- **Updating Network Settings after a NIC Replacement**

Before you begin, review the guidelines for navigating the installation wizard. See **Using the Installation Wizard**.

CAUTION

Changing the network settings of a host in an HA cluster causes HA to cease functioning on the cluster. If you want to change the network settings of a host in an HA cluster, you must first remove the host from the cluster, make your changes, and then re-add the host to the cluster.

Changing 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.

To change the settings on the QRadar SIEM Console:

NOTE

You must have a local connection to your Console before executing the script.

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.

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

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

Step 5 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 8**.
- If you are using 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 To 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. 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.
- **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.

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 non-Console managed hosts from the deployment, change the network settings, re-add the managed host or hosts, and then re-assign the component or components.

You must perform this procedure in the following order:

1. **Removing Non-Console Managed Hosts**
2. **Changing the Network Settings**
3. **Re-Adding Managed Hosts and Re-Assigning the Components**

NOTE

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

Removing Non-Console Managed Hosts

To remove non-Console managed hosts from your deployment, you must:

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.

The deployment editor is displayed.

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

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

Repeat for each non-Console managed host until all hosts are deleted.

Step 6 Click **Save**.

Step 7 Close the deployment editor.

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

The changes are deployed.

Changing the Network Settings

To change the network settings, you must:

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.

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

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

Step 5 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 8**.
- If you are using 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 To 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. 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.
- **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.

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.

Re-Adding Managed Hosts and Re-Assigning the Components

To re-add the managed hosts and re-assign components, you must:

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**.

The Add a new host wizard is displayed.

Step 6 Click **Next**.

The Enter the host's IP window is displayed.

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.

  The password must meet the following criteria:

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

NOTE

You can also right-click a component to access the Actions menu items.

The Assign Component wizard is displayed.

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**.

The changes are deployed.

Changing the Network Settings of a Non-Console in a Multi-System Deployment

To change the network settings of a non-Console in a multi-system deployment, you must remove the non-Console 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.

You must perform this procedure in the following order:

- **Removing the Non-Console Managed Host**
- **Changing the Network Settings**
- **Re-Adding the Managed Host and Re-Assigning the Components**

NOTE

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

Removing the Non-Console Managed Host

To remove non-Console managed host from your deployment, you must:

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.

The deployment editor is displayed.

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**.

The changes are deployed.

Changing the Network Settings

To change the network settings, you must:

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 depending on your hardware configuration. Each interface with a physical link is denoted with a plus (+) symbol.

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

Step 5 Choose one of the following options:

- If you are using IPv4 as your Internet protocol, go to **Step 8**.
- If you are using 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 To 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. 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.
- **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.

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.

Re-Adding the Managed Host and Re-Assigning the Components

To re-add the managed host and re-assign components, you must:

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.

The deployment editor is displayed.

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

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

The Add a new host wizard is displayed.

Step 6 Click **Next**.

The Enter the host’s IP window is displayed.

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.

The password must meet the following criteria:

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

- **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**.

NOTE

You can also right-click a component to access the **Actions** menu items.

The Assign Component wizard is displayed.

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**.

The changes are deployed.

Updating Network Settings after a NIC Replacement

The hardware in your QRadar SIEM deployment can include motherboards with integrated Network Interface Cards (NIC) or stand-alone NICs. These procedures only apply to replacements of integrated motherboards and stand-alone NICs.

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.

After you replace your integrated motherboard or NIC, reboot your QRadar SIEM system and update the network settings.

To reboot and update your network settings:

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 Edit the network settings file by typing the following command:

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

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.

The output may resemble the following:

```
# 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.

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
```

Your network settings are now updated.

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