IBM Security QRadar
Version 7.1.0 (MR1)

High Availability Guide

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

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar High Availability (HA) Guide* provides information on how to protect your QRadar data by implementing an HA solution.

Unless otherwise noted, all references to QRadar refer to IBM Security QRadar SIEM and IBM Security QRadar Log Manager.

Intended Audience

This guide is intended for all QRadar users responsible for managing high availability. This guide assumes that you have QRadar access and a knowledge of your corporate network and networking technologies.

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 QRadar High Availability

In the event of a hardware or network failure, High Availability (HA) ensures that QRadar continues to collect, store, and process data.

Unless otherwise noted, all references to QRadar refer to IBM Security QRadar SIEM and IBM Security QRadar Log Manager.

This section includes the following topics:

High Availability Overview

To enable HA, QRadar connects a primary HA host with a secondary HA host to create an HA cluster. The secondary HA host maintains the same data as the primary HA host by one of two methods: data synchronization or shared external storage. If the secondary HA host detects a failure, it automatically assumes all the responsibilities of the primary HA host.

Scenarios that cause failover include:

- Network failure that is detected by network connectivity testing.

  For more information, see **Network Connectivity Tests**.
- Management interface failure on the primary HA host.
- Complete Redundant Array of Independent Disks (RAID) failure on the primary HA host.
- Power supply failure.
- Operating system malfunction that delays or stops the heartbeat ping.

  For more information, see **Heartbeat Ping Tests**.
- Manual failover.

QRadar HA does not protect against software errors. The scenarios that do not cause an automatic failover of your primary HA host include:

- If any QRadar processes develop an error, stop functioning or exit with an error, the HA process will not detect this and your primary HA host will not failover.
- If a disk on your primary HA host reaches 95%, QRadar data collection processes will shut down, but the primary HA host will not failover.

HA Clustering

An HA cluster consists of a primary HA host, secondary HA host, and cluster virtual IP address. You can configure the HA cluster using the QRadar user interface.

This section includes the following topics:

- **Primary HA host**
- **Secondary HA Host**
- **Cluster Virtual IP Address**

Primary HA host

The primary HA host is any console or managed host in your QRadar deployment that requires protection from data loss in the event of a failure. When you configure HA, the IP address of the primary HA host is automatically reassigned to a cluster virtual IP address. Therefore, you must assign a new, unused IP address to the primary HA host. For more information, see **Adding an HA Cluster**.

Secondary HA Host

The secondary HA host is the standby system for the primary HA host. If the primary HA host fails, the secondary HA host automatically assumes all the responsibilities of the primary HA host.

Cluster Virtual IP Address

If the primary HA host fails, the cluster virtual IP address is assumed by the secondary HA host. QRadar uses the cluster virtual IP address to allow other hosts in your deployment to continue communicating with the HA cluster without requiring you to reconfigure the hosts to send data to a new IP address.

Data Storage Strategies

To ensure that the hosts in an HA cluster maintain access to the same data, QRadar provides two HA data storage strategies.

This section includes the following topics:

- **Disk Synchronization**
- **Shared Storage**

Disk Synchronization

In an HA enviornment, data synchronization is performed in the following scenarios:

- When you initially configure an HA cluster.
- During normal HA operation, data is synchronized in real-time between the primary and secondary HA hosts.
- When a primary HA host is restored after a failover.

HA Cluster Synchronization

If the primary HA host /store partition is not mounted to an external storage device and you configure an HA cluster, the /store file system on the primary HA host is automatically synchronized with the /store partition on the secondary HA host using Distributed Replicated Block Device (DRBD). After synchronization is complete, the secondary HA host assumes a status of Standby. For more information on the status of the hosts in your HA cluster, see **Adding an HA Cluster**.

NOTE

DRBD is not enabled by default for IBM Security QRadar QFlow Collectors. To synchronize QRadar QFlow data, you must configure an HA cluster using the console or managed host that is collecting QRadar QFlow data.

When you initially configure an HA cluster, disk synchronization can take an extended period of time, depending on the size of the primary /store partition and the disk synchronization speed. Ensure that the connection between the primary and secondary HA host has a minimum bandwidth of 1 gigabits per second(Gbps).

Post-Failover Synchronization

Data collected by a primary HA host up to the point of failover is maintained virtually in real-time with the secondary HA host using DRBD. When the primary HA host is restored, only the data collected by the secondary HA host in the intervening period is synchronized with the primary HA host.

Therefore, the period of time taken to perform post-failover disk synchronization is considerably less than the initial disk synchronization, unless the disk on the primary HA host was replaced or reformatted when the host was manually repaired.

When restored from a failover, the primary HA host assumes a status of offline. You must set the primary HA host to the online state before it becomes the Active host. Disk replication with the secondary HA host is enabled while the primary HA host remains offline. For more information on setting the primary HA host online, see **Setting an HA Host Online**.

Shared Storage

If you are implementing HA on a primary HA host that has the /store partition mounted to an external storage solution, review the following information:

- Do not create an HA cluster using the QRadar user interface until you have configured the secondary HA host to access the external storage device. For more information, see the *IBM Security QRadar Offboard Storage Guide.*
- Before you make changes to your external storage device configuration on an HA cluster you must remove the HA cluster between the primary and secondary HA host. For more information, see **Editing an HA Cluster**
- During an upgrade to QRadar 7.1, reconfigure the external storage device connections to the primary and secondary HA host in your HA cluster. For more information, see the *Reconfiguring Offboard Storage During a QRadar Upgrade Technical Note.*

HA Failovers

Failover occurs when the primary HA host experiences a failure, loses network connectivity, or if you perform a manual failover. During failover, the secondary HA host assumes the responsibilities of the primary HA host by performing the following actions in sequence:

1. If configured, external shared storage devices are detected and the file systems are mounted. For more information, see the *IBM Security QRadar Offboard Storage Guide*.
2. A management interface network alias is created. For example, the network alias for eth0 is eth0:0.
3. The cluster virtual IP address is assigned to the network alias.
4. All QRadar services are started.
5. The secondary HA host connects to the console and downloads configuration files.

This section includes the following topics:

- **Primary Network Failures**
- **Primary Disk Failure**
- **Secondary HA Host Network or Disk Failure**
- **Manual Failovers**

Primary Network Failures

A primary HA host fails if the HA network connectivity or heartbeat ping tests identify a communication problem with the HA cluster.

Network Connectivity Tests

To test network connectivity, the primary HA host automatically pings all existing managed hosts in the QRadar deployment. If the primary HA host loses network connectivity to a managed host, but the connection to the secondary HA host remains intact, the secondary HA host performs another network connectivity test with the managed hosts. If the test succeeds, the primary HA host performs a

controlled failover to the secondary HA host. If the test fails, HA failover is not performed because the secondary HA host might also be experiencing network connectivity problems.

For more information on configuring HA network connectivity tests, see the advanced HA options listed in **Table 1-2**.

Heartbeat Ping Tests

A preconfigured intervals, the secondary HA host sends a heartbeat ping to the primary HA host. If the secondary HA host does not receive a response from the primary HA host within the preconfigured time period, the primary HA host is considered to be unavailable and automatic failover to the secondary is performed.

For more information on configuring heartbeat pings, see the options listed in **Table 1-2**.

Primary Disk Failure

An HA cluster configured with DRBD, monitors disks on which the /store partition is mounted. If RAID completely fails and all disks are unavailable, the primary HA host performs a shut down and fails over to the secondary HA host. After a failover, the primary HA host assumes a status of Failed. For more information on the status of the hosts in your HA cluster, see **Adding an HA Cluster**.

Secondary HA Host Network or Disk Failure

If the primary HA host detects that the secondary HA host has failed, the primary HA host generates an event to indicate that the secondary HA host is no longer providing HA protection.

Manual Failovers

You can manually force a failover from a primary HA host to a secondary HA host. This is useful for planned hardware maintenance on the console or managed host. Before you perform a failover, the primary and secondary HA hosts must be synchronized and the secondary HA host must display a status of Standby.

To perform hardware maintenance on a primary and secondary HA host while the secondary HA host is in Standby, set the secondary HA host offline and power off the primary HA host. If the primary and secondary HA hosts are synchronizing, power off the primary.

For more information on manually forcing a failover, see **Setting an HA Host Offline**.

CAUTION

Do not manually force a failover on a primary HA host when you install patches or perform software upgrades. For more information, see the IBM Security QRadar SIEM Upgrade Guide or the *IBM Security QRadar Log Manager Upgrade Guide.*

2 PLANNING YOUR HIGH AVAILABILITY DEPLOYMENT

Before you implement HA in your IBM Security QRadar deployment, plan your implementation by reviewing the required network and software configurations.

This section includes the following topics:

Architecture Considerations

This section includes the following topics:

Appliance Recommendations

Before adding a secondary HA host to an HA cluster, review the following:

- The build version of the secondary HA host must be greater than or equal to the QRadar build version installed on the primary HA host.
- The patch level of the secondary HA host must be less than or equal to the patch level of the primary HA host.

  When you configure an HA cluster, the HA configuration process patches the secondary HA host to the same level as the primary HA host.
- Ensure the secondary HA host that you want to add to the HA cluster has a valid HA activation key.

IP Addressing and Subnets

Virtual LAN (VLAN) routing is not recommended. Ensure that:

- The secondary HA host is located on the same subnet as the primary HA host.
- When the primary HA host IP address is reassigned as a cluster virtual IP, the new IP address that you assign to the primary HA host is located on the same subnet.

  For more information about HA virtual clusters, see **HA Clustering**.
- The secondary HA host that you want to add to the HA cluster must not be a component in another HA cluster.

Management Interfaces and Ports

Before configuring an HA cluster, review the following information:

- The management interface supports one cluster virtual IP address. Multihoming is not supported.
- The secondary HA host must use the same management interface as the primary HA host. For example, if the primary HA host uses ETH0 as the management interface, the secondary HA host must also use ETH0.
- DRBD uses an assigned port number that supports bi-directional communication between the primary and secondary HA host. For more information on the assigned port number, see the *QRadar Common Ports List Technical Note*.

Storage Recommendations

If you configure HA on your own hardware that is installed with QRadar software, the size of the /store partition on the secondary HA host must be equal to or larger than the /store partition on the primary HA host. For example, do not pair a primary HA host that uses a 3 TB disk with a secondary HA host that uses a 2 TB disk. The appliances must be the same model and type, and have the same disk configuration.

Link Bandwidth and Latency

If your HA cluster is using disk synchronization, see **Disk Synchronization**, ensure that:

- The connection between the primary and secondary HA host has a minimum bandwidth of 1 gigabits per second (Gbps).
- The latency between the primary and secondary HA host is less than 2 milliseconds (ms).

NOTE

If your HA solution uses a wide area network (WAN) to geographically distribute the hosts in your cluster, latency will increase with distance. If latency rises above 2 ms, system performance will be affected.

Backup Considerations

We recommend that you backup your configuration information and data on all hosts you intend to configure for HA. For more information on backing up your configuration information and data, see the *IBM Security QRadar SIEM Administration Guide or* the *IBM Security QRadar Log Manager Administration Guide*.

If a backup archive originates on an HA cluster, click **Deploy Full Configuration** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary HA host immediately synchronizes data after the system is restored. If the secondary HA host was removed from the deployment after backup was performed, the secondary HA host displays a Failed status on the System and License Management window. For more information on restoring backup archives in an HA environment, see the *IBM Security QRadar SIEM Administration Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

Storage Solution Considerations

To ensure that data is protected, QRadar provides two HA storage solutions: disk synchronization and external offboard storage.

This section includes the following topics:

- **Offboard Storage Solutions**
- **Disk Synchronization**

Offboard Storage Solutions

If you implement an external storage solution, the data received by the primary HA host is migrated to an external disk, but remains accessible to the primary HA host for searching and reporting purposes. For example, if you deploy an iSCSI device, the /store partition is unmounted from the local disk and remounted to an external device.

In an HA deployment, if the primary HA host fails over, the /store partition on the secondary HA host is automatically mounted to the external device, where it continues to read and write to the data received by the primary HA host before failover.

Before you implement HA with an external storage solution, review the following information:

- The primary HA host must be configured to communicate with the external device and the data in the /store partition of the local disk migrated to the external device.
- The secondary HA host must be configured to communicate with the external device, so that when a primary HA host fails over, the secondary HA host automatically detects the external storage device.

  For more information on configuring your primary and secondary HA hosts in an HA environment with offboard storage, see the *IBM Security QRadar Offboard Storage Guide*.
- Ensure that there is at least a 1 Gbps connection between each HA host and your external device.

Disk Synchronization

If you do not choose an offboard storage solution, the data on the /store partition of the primary HA host is written to local disk and replicated in real-time with the local disk on the secondary HA host.

During disk synchronization when the primary HA host is active, the /store file system on the secondary HA host is not mounted to its local disk. The QRadar replication process maintains synchronization by using DRBD virtual disks on both the primary and secondary HA hosts.

In an HA deployment, if the primary HA host fails over, the /store file system on the secondary HA host is automatically mounted to its local disk, where it continues to read from and write to the data received by the primary HA host before the failover.

NOTE

Disk replication is not enabled by default on QRadar QFlow Collectors and is not required for successful failover.

3 INSTALLING OR RECOVERING QRADAR HA APPLIANCES

This section provides information on installing or recovering your IBM Security QRadar High Availability (HA) appliances.

This section includes the following topics:

Reinstalling QRadar on a Failed Primary HA Host Failure

If the primary HA host in an HA cluster fails and requires reinstallation of QRadar, review the following:

- The build version of the primary HA host must be greater than or equal to the QRadar build version installed on the secondary HA host.
- The patch level of the primary HA host must be less than or equal to the patch level of the secondary HA host.

  When you configure an HA cluster, the HA configuration process patches the primary HA host to the same level as the secondary HA host.

Installing or Recovering a Secondary HA QRadar Console Appliance

To install or recover your secondary HA QRadar appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

For information on your QRadar appliance, see the *IBM Security QRadar Hardware 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 *IBM Security QRadar Hardware 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 press Enter.

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

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 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 **Host Name** field. For more information on managing HA, see **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 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. For more information, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 11 To configure the QRadar root password:

a Type your password.

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 continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

e Press Enter to select **OK**.

Step 12 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide or the IBM Security QRadar Log Manager Installation Guide*.

Step 13 Configure your HA cluster. For more information on configuring your HA cluster, see **Adding an HA Cluster**.

Installing or Recovering a Secondary HA QRadar Non Console Appliance

To install or recover your secondary HA QRadar QFlow appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

For information on your QRadar appliance, see the *IBM Security QRadar Hardware 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 *IBM Security QRadar Hardware 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 press Enter.

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

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 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 **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 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 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 continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 9 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 10 Configure your HA cluster. For more information on configuring your HA cluster, see **Adding an HA Cluster**.

Recovering a Failed Primary HA QRadar Appliance

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

- Cluster Virtual IP Address
- Primary IP Address

You can display these IP addresses in the System and License Management window by hovering your mouse over the **Host Name** field. For more information on the System and License Management window, see the *IBM Security QRadar SIEM Administration Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

CAUTION

If your HA cluster uses shared storage, you must manually configure your external storage device. For more information, see the IBM Security QRadar Offboard Storage Guide.

To recover a failed primary HA QRadar appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

For more information on your QRadar appliance, see the *IBM Security QRadar Hardware 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 *IBM Security QRadar Hardware 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 press Enter.

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

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 hovering your mouse over the **Host Name** field.

Step 11 Configure the QRadar 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 **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 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 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 is displayed as QRadar continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 13 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 14 Restore the failed primary HA host. For more information on restoring a failed primary HA host, see **Restoring a Failed Host**.

Recovering a Failed Secondary HA Host to the QRadar 7.1

When recovering a failed secondary HA host that used a previous QRadar version, you can install QRadar 7.1 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 software from the Qmmunity website.

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

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

CAUTION

If you are installing QRadar *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. 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, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

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

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 user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can display these IP addresses in the System and License Management window by hovering your mouse over the **Host Name** field. For more information on the System and License Management window, see the *IBM Security QRadar SIEM Administration Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

CAUTION

If your HA cluster uses shared storage, you must manually configure your external storage device. For more information, see the IBM Security QRadar Offboard Storage Guide.

To recover a failed primary HA QRadar QFlow appliance:

Step 1 Prepare your appliance.

a Install all necessary hardware.

For more information on your QRadar appliance, see the *IBM Security QRadar Hardware 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 *IBM Security QRadar Hardware 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 press Enter.

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

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 hovering your mouse over the **Host Name** field.

Step 8 Configure the QRadar 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 hovering your mouse over the **Host Name** field. For more information on managing HA, see **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 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 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 continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 10 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 11 Restore the failed primary HA host. For more information on restoring a failed primary HA host, see **Restoring a Failed Host**.

Installing or Recovering QRadar Console Software On Your Secondary HA System

To install or recover QRadar Console software on your secondary HA system:

Step 1 Install the necessary hardware.

Step 2 Obtain the Red Hat Enterprise Linux 6.2 operating system and install it on your hardware.

For instructions on how to install and configure the Red Hat Enterprise Linux 6.2 operating system, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 3 Log in as root.

Step 4 Create the /media/cdrom directory by typing the following command:

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar software from the Qmmunity website.

Step 6 Mount the QRadar 7.1 ISO by typing the following command:

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

Step 7 Begin the installation by typing the following command:

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

NOTE

QRadar verifies the integrity of the media before installation by checking the MD5 sum. If a warning message is displayed that the MD5 checksum failed, redownload QRadar and start over. 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 press Enter.

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

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 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 Secondary 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 **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 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. For more information, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 19 To configure the QRadar root password:

a Type your password.

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 continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

e Press Enter to select **OK**.

Step 20 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 21 Configure your HA cluster. For more information on configuring your HA cluster, see **Adding an HA Cluster**.

Installing or Recovering QRadar Non-Console Software On Your Secondary HA System

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

Step 1 Install the necessary hardware.

Step 2 Obtain the Red Hat Enterprise Linux 6.2 operating system and install it on your hardware.

For instructions on how to install and configure the Red Hat Enterprise Linux 6.2 operating system, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 3 Log in as root.

Step 4 Create the /media/cdrom directory by typing the following command:

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar software from the Qmmunity website.

Step 6 Mount the QRadar 7.1 ISO by typing the following command:

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

Step 7 Begin the installation by typing the following command:

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

NOTE

QRadar verifies the integrity of the media before installation by checking the MD5 sum. If a warning message is displayed that the MD5 checksum failed, you will be required to re-download or re-burn QRadar. 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 press Enter.

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

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 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 **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 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 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** option and press Enter.

A series of messages are displayed as QRadar continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 17 Log in to the QRadar user interface. For more information, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 18 Configure your HA cluster. For more information on configuring your HA cluster, see **Adding an HA Cluster**.

Recovering QRadar 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 user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by hovering your mouse over the **Host Name** field. For more information on the System and License Management window, see the *IBM Security QRadar SIEM Administration Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

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 6.2 operating system and install it on your hardware.

For instructions on how to install and configure the Red Hat Enterprise Linux 6.2 operating system, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 3 Log in as root.

Step 4 Create the /media/cdrom directory by typing the following command:

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar software from the Qmmunity website.

Step 6 Mount the QRadar 7.1 ISO by typing the following command:

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

Step 7 Begin the installation by typing the following command:

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

NOTE

QRadar verifies the integrity of the media before installation by checking the MD5 sum. If a warning message is displayed, that the MD5 checksum failed, redownload QRadar. 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 press Enter.

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

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 hovering your mouse over the **Host Name** field.

Step 19 Configure the QRadar 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 hovering your mouse over the **Host Name** field. For more information on the System and License Management window, see

- **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 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 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 is displayed as QRadar continues with the installation. This process can take several minutes.

The Configuration is Complete window is displayed.

c Press Enter to select **OK**.

Step 21 Log in to the QRadar user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 22 Restore the failed primary HA host. For more information on restoring a failed primary HA host, see **Restoring a Failed Host**.

Recovering QRadar 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 user interface:

- Cluster Virtual IP Address
- Primary IP Address

NOTE

You can find these IP addresses in the System and License Management window by hovering your mouse over the **Host Name** field. For more information on the System and License Management window, see the *IBM Security QRadar SIEM Administration Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

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 6.2 operating system and install it on your hardware.

For instructions on how to install and configure the Red Hat Enterprise Linux 6.2 operating system, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 3 Log in as root.

Step 4 Create the /media/cdrom directory by typing the following command:

```
mkdir /media/cdrom
```

Step 5 Obtain the QRadar software from the Qmmunity website.

Step 6 Mount the QRadar 7.1 ISO by typing the following command:

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

Step 7 Begin the installation by typing the following command:

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

NOTE

QRadar verifies the integrity of the media before installation by checking the MD5 sum. If a warning is displayed that the MD5 checksum failed, you should re-download or re-burn QRadar. 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 press Enter.

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

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 hovering your mouse over the **Host Name** field.

Step 16 Configure the QRadar 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 hovering your mouse over the **Host Name** field. For more information on managing HA, see **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 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 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 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 user interface. See the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

Step 19 Restore the failed primary HA host. For more information on restoring a failed primary HA host, see **Restoring a Failed Host**.

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

Using this procedure, you can recover a failed QRadar 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 version you want to restore.

Step 4 Using SCP, copy the ISO to the target QRadar 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. 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, see the *IBM Security QRadar SIEM QRadar Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.

4 MANAGING HIGH AVAILABILITY

Using the System and License Management window, you can manage and configure your HA deployment.

This section includes the following topics:

Adding an HA Cluster

An HA Cluster is established when a primary (console or non-console) host, secondary HA host, and a virtual IP address are paired using the IBM Security QRadar user interface.

CAUTION

If a primary HA host is configured with external storage, you must configure the secondary HA host with the same external storage options before attempting to establish an HA cluster. For more information, see the IBM Security QRadar Offboard Storage Guide.

To add an HA cluster:

Step 1 Click the **Admin** tab.

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

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

The System and License Management window is displayed.

Step 4 Select the host for which you want to configure HA.

Step 5 From the **Actions** menu, select **Add HA Host**.

If the primary HA host is a Console, a warning message is displayed to indicate that the QRadar user interface restarts after you establish the HA cluster. Click **OK**.

The HA Wizard is displayed.

NOTE

If you do not want to view the Welcome to the High Availability Wizard page again, select the **Skip this page when running the High Availability wizard** check box.

Step 6 Read the introductory text. Click **Next**.

Step 7 To configure the HA host information, configure the following parameters:

Table 1-1 HA Host Information Parameters

Parameter	Description
Primary HA host IP Address	Type a new primary HA host IP address. The new primary HA host IP address is assigned to the primary HA host, replacing the previous IP address. The current IP address of the primary HA host becomes the Cluster Virtual IP address. If the primary HA host fails and the secondary HA host becomes active, the Cluster Virtual IP address is assigned to the secondary HA host. The new primary HA host IP address must be on the same subnet as the virtual Host IP.
Secondary HA host IP Address	Type the IP address of the secondary HA host that you want to add. The secondary HA host must be in the same subnet as the primary HA host.
Enter the root password of the host	Type the root password for the secondary HA host. The password must not include special characters.
Confirm the root password of the host	Type the root password for the secondary HA host again for confirmation.

Step 8 Optional. To configure advanced parameters:

a Click the arrow beside **Show Advanced Options**.

b Configure the following parameters:

Table 1-2 Advanced Options Parameters

Parameter	Description
Heartbeat Interval (seconds)	Type the time, in seconds, that you want to elapse between heartbeat pings. The default is 10 seconds. At the specified interval, the secondary HA host sends a heartbeat ping to the primary HA host to detect hardware and network failure. For more information on heartbeat pings, see **Heartbeat Ping Tests**.

Table 1-2 Advanced Options Parameters (continued)

Parameter	Description
Heartbeat Timeout (seconds)	Type the time, in seconds, that you want to elapse before the primary HA host is considered unavailable if no heartbeat detected. The default is 30 seconds. If the secondary HA host detects a failure, the secondary HA host automatically assumes all the responsibilities of the primary HA host. For more information on failover scenarios, see **HA Failovers**.
Network Connectivity Test List peer IP addresses (comma delimited)	Type the IP addresses of the hosts you want the secondary HA host to ping, in order to test its own network connection. The default is all other managed hosts in the QRadar deployment. For more information on network connectivity testing, see **Primary Network Failures**.
Disk Synchronization Rate (MB/s)	Type or select the disk synchronization rate. The default is 100 MB/s. When you initially add an HA cluster, the first disk synchronization can take an extended period of time to complete, depending on size of your /store partition and your disk synchronization speed. For example, initial disk synchronization can take up to 24 hours or more. The secondary HA host only assumes the Standby status after the initial disk synchronization is complete. Ensure that the connection between the primary HA host and secondary HA host has a minimum bandwidth of 1 gigabits per second (Gbps).
Disable Disk Replication	Select this option if you want to disable disk replication. This option is only displayed if you are configuring an HA cluster using a managed host.

c Click **Next**.

The Confirm the High Availability Wizard options page is displayed.

NOTE

If required, click **Back** to return to the Confirm the High Availability Wizard Options page to edit the parameters you selected.

Step 9 Review the information. Click **Finish**.

The HA Wizard connects the primary and secondary HA host and performs the following validation:

- Verifies that the secondary HA host has a valid HA activation key.
- Verifies that the secondary HA host is not part of another HA cluster.

- Verifies that the software versions on the primary and secondary HA hosts are the same.
- Detects if the primary HA host is configured with an external storage device. If successful, the HA wizard attempts to verify that the secondary HA host has been configured to access the same external storage device.
- Verifies that the primary and secondary HA hosts support the same Device Support Module (DSM), scanner, and protocol RPMs.

If any validation test fails, the HA wizard displays an error message and closes.

NOTE

If Disk Synchronization is enabled, it can take 24 hours or more for the data on the primary HA host /store partition to initially synchronize with the HA secondary HA host.

The System and License Management window displays the HA cluster that you added. Use the **Arrow** icon to display or hide the secondary HA host.

The System and License Management window displays the status of each host as the HA cluster is established, including:

Table 1-3 HA Status Descriptions

Status	Description
Active	Specifies that the host is the active system with all services running. Either the primary or secondary HA host can display the Active status. If the secondary HA host is displaying the Active status, the primary HA host has failed.
Standby	Specifies that the host is acting as the standby system. This status is only displayed for a secondary HA host. The standby system has no services running. If disk replication is enabled, the standby system replicates data from the primary HA host. If the primary HA host fails, the standby system automatically assumes the active status.

Table 1-3 HA Status Descriptions (continued)

Status	Description
Failed	Specifies that the host has failed. Both the primary or secondary HA host can display the Failed status: • If the primary HA host displays the Failed status, the secondary HA host assumes the responsibilities of the primary HA host and displays the Active status. • If the secondary HA host displays the Failed status, the primary HA host remains active, but is not protected by HA. A system in a failed state must be manually repaired or replaced, and then restored. See **Restoring a Failed Host**. ***Note:*** *Depending on the type of failure that caused the failover, you may not be able to access a failed system from the Console.*
Synchronizing	Specifies that data is synchronizing between hosts. For more information on data synchronization, see **Disk Synchronization** ***Note:*** *This status is only displayed if disk replication is enabled.*
Online	Specifies that the host is online.
Offline	Specifies that the host is offline. All processes are stopped and the host discontinues monitoring the heartbeat of the active system. Both the primary and the secondary can display the offline status. While in the offline state, disk replication continues if it is enabled.
Restoring	If you select **High Availability > Restore System** to restore a failed host, this status specifies that the system is in the process of restoring. For more information, see **Restoring a Failed Host**
Needs License	Specifies that a license key is required for the HA cluster. In the Needs License state, no processes are running. For more information on applying a license key, see the *IBM Security QRadar SIEM Administration Guide or the* or the *IBM Security QRadar Log Manager Administration Guide*.
Setting Offline	Specifies that the host is in the process of changing status from online to offline.
Setting Online	Specifies that the host is in the process of changing status from offline to online.

Table 1-3 HA Status Descriptions (continued)

Status	Description
Needs Upgrade	Specifies that the host requires a software upgrade, because the primary HA host has been upgraded to a newer software version. If the secondary HA host displays the Needs Upgrade status, the primary HA host remains active, but is not protected by HA. Heartbeat monitoring and disk replication, if enabled, continue to function. ***Note:*** *Only a secondary HA host can display a Needs Upgrade status.*
Upgrading	Specifies that the host is in the process of upgrading software. If the secondary HA host displays the Upgrading status, the primary HA host remains active, but is not protected by HA. Heartbeat monitoring and disk replication, if enabled, continue to function. ***Note:*** *After DSMs or protocols are installed on a Console and the new configurations are deployed, the Console replicates the DSM and protocol updates to its managed hosts. When primary and secondary HA hosts are synchronized, the DSM and protocols updates are installed on the secondary HA host.* ***Note:*** *Only a secondary HA host can display an Upgrading status.*

NOTE

When an HA cluster has been configured, you can display the IP addresses that are used in the HA cluster by hovering your mouse over the **Host Name** field on the System and License Management window.

Editing an HA Cluster

Using the Edit HA Host feature, you can edit the advanced options for your HA cluster.

To edit an HA cluster:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the row for the HA cluster that you want to edit.

Step 5 From the **High Availability** menu, select **Edit HA Host**.

The HA Wizard is displayed.

Step 6 Edit the parameters in the advanced options section. See **Table 1-2**.

Step 7 Click **Next**.

Step 8 Review the information. Click **Finish**.

The secondary HA host restarts and your HA cluster continues functioning.

Setting an HA Host Offline

You can set either the primary or secondary HA host to Offline from the Active or Standby state. If you set the active system to Offline, the standby system becomes the active system, thereby forcing a failover. If you set the standby system to Offline, the standby system no longer monitors the heartbeat of the active system, however, continues to synchronize data from the active system.

To set an HA host offline:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the HA host that you want to set to offline.

Step 5 From the **High Availability** menu, select **Set System Offline**.

The status for the host changes to Offline.

Setting an HA Host Online

When you set the secondary HA host to Online, the secondary HA host becomes the standby system. If you set the primary HA host to Online while the secondary system is Active, the primary HA host becomes the active system and the secondary HA host automatically becomes the standby system.

To set an HA host online:

Step 1 Click the **Admin** tab.

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

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

Step 4 Select the offline HA host that you want to set to Online.

Step 5 From the **High Availability** menu, select **Set System Online**.

The status for the host changes to Online.

If you experience a problem setting a host Online, see **Troubleshooting QRadar High Availability**.

Restoring a Failed Host

If a host displays a status of Failed or Unknown, troubleshoot your HA cluster. For more information, see **Troubleshooting QRadar High Availability**.

5 TROUBLESHOOTING QRADAR HIGH AVAILABILITY

When an HA cluster is configured, the System and License Management window displays the status of both the primary and secondary HA host. For more information on the status that is displayed, see **Adding an HA Cluster**.

If the System and License Management window displays a primary and secondary HA host status that is listed in **Table 1-4**, troubleshoot your HA cluster.

Table 1-4 System and License Management Window Host Statuses

Primary HA Host Status	Secondary HA Host Status
Active	Failed or Unknown
Failed or Unknown	Active
Unknown	Unknown
Offline	Active

This section includes the following topics:

Active Primary HA Host and Failed Secondary HA Host

If the secondary HA host displays a status of Unknown or Failed, verify that the host is operational, and then restore the secondary HA host.

This section includes the following topics:

Verifying that the Secondary HA Host Is Operational

To verify that the secondary HA host is operational:

Step 1 Using SSH, log in to the Secondary HA Host as the root user:

Username: `root`

Password: `<password>`

Step 2 Choose one of the following options:

- If you can connect to the secondary HA host using SSH, restore the secondary HA host. See **Restoring a Failed Secondary HA Host**.
- If you cannot connect to the secondary HA host using SSH:
  - If you have Dell Remote Access Controller (DRAC) access to the secondary HA host, ensure that the secondary HA host is on.
  - If the secondary HA host is on, or you do not have DRAC access to the system, contact Customer Support for further assistance.

Restoring a Failed Secondary HA Host

To restore a secondary HA host:

Step 1 Click the **Admin** tab.

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

Step 3 Click **System and License Management**.

Step 4 Select the secondary HA host that you want to restore.

Step 5 From the **High Availability** menu, select **Restore System**.

While the HA configuration is restored, the status of the secondary HA host displays the following in sequence:

a Restoring

b Synchronizing (if disk synchronization is enabled)

c Standby

Step 6 Verify the status of the secondary HA host on the System and License Management window. Choose one of the following options:

- If the secondary HA host displays a status of Standby, you have restored the secondary HA host.
- If the secondary HA host displays a status of Failed or Unknown, go to **Step 7**.
- If you repeatedly attempt to restore the secondary HA host and the System and License Management window displays a status of Failed or Unknown, contact Customer Support for further assistance.

Step 7 Using SSH, log in to the Secondary HA Host as the root user:

Username: `root`

Password: `<password>`

Step 8 Restart the secondary HA host by typing the following command:

```
reboot
```

Step 9 After the system is restarted, verify the status of the secondary HA host on the System and License Management window. Choose one of the following options:

- If the secondary HA host displays a status of Standby, you have restored the secondary HA host.
- If the secondary HA host displays a status of Failed or Unknown, repeat **Step 5**.

Failed Primary HA Host and Active Secondary HA Host

If the primary HA host displays a status of Unknown or Failed, verify that the host is operational, and then restore the primary HA host.

This section includes the following topics:

- **Verifying that the Primary HA Host Is Operational**
- **Restoring a Failed Primary HA Host**

Verifying that the Primary HA Host Is Operational

To verify that the primary HA host is operational:

Step 1 Using SSH, log in to the Primary HA Host as the root user:

Username: `root`

Password: `<password>`

Step 2 Choose one of the following options:

- If you can connect to the primary HA host using SSH, restore the primary HA host. See **Restoring a Failed Primary HA Host**.
- If you cannot connect to the primary HA host using SSH:
  - If you have Dell Remote Access Controller (DRAC) access to the primary HA host, ensure that the primary HA host is on.
  - If the primary HA host is on, or you do not have DRAC access to the system, contact Customer Support for further assistance.

Restoring a Failed Primary HA Host

To restore a primary HA host:

Step 1 Click the **Admin** tab.

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

Step 3 Click **System and License Management**.

Step 4 Select the primary HA host that you want to restore.

Step 5 From the **High Availability** menu, select **Restore System**.

While the HA configuration is restoring, the status of the primary HA host displays the following in sequence:

a Restoring

b Synchronizing (if disk synchronization is enabled)

c Offline

Step 6 Verify the status of the primary HA host on the System and License Management window. Choose one of the following options:

- If the primary HA host displays a status of Offline, go to **Step 7**.
- If the primary HA host displays a status of Failed or Unknown, go to **Step 9**.

Step 7 From the System and License Management window, select **High Availability > Set System Online**.

Step 8 On the System and License Management window, verify the status of the primary HA host. Choose one of the following options:

- If the primary HA host displays a status of Active, you have restored the primary HA host.
- If the primary HA host displays a status of Offline, contact Customer Support for further assistance.
- If the primary HA host displays a status of Failed or Unknown, go to **Step 9**.
- If you repeatedly attempt to restore or set the primary HA host Online and the System and License Management window displays a status of Failed, Unknown, or Offline, contact Customer Support for further assistance.

Step 9 Using SSH, log in to the primary HA host as the root user:

Username: `root`

Password: `<password>`

Step 10 Restart the primary HA host by typing the following command:

```
reboot
```

Step 11 On the System and License Management window, verify the status of the primary HA host. Choose one of the following options:

- If the primary HA host displays a status of Offline, go to **Step 7**.
- If the primary HA host displays a status of Failed or Unknown, repeat **Step 5**.

Unknown Status for Both Primary and Secondary HA Hosts

On the System and License Management window, if the status of both the primary and secondary HA host is Unknown, identify which host was Active before each HA host displayed a status of Unknown. The most recent QRadar data is maintained on the HA host that was last Active.

NOTE After you identify the most recently Active HA host, contact Customer Support for assistance with restoring your HA cluster.

This section includes the following topics:

Verifying that the Primary and Secondary HA Hosts are Operational

Before you troubleshoot a primary and secondary HA host that displays a status of Unknown in the System and License Management window, you must identify if the primary HA host was configured as a Console or managed host.

Choose from one of the following options:

- If your primary HA host was configured as a Console, go to **Step 1**.
- If you primary HA host was configured as a managed host, go to **Step 2**.

Step 1 Using SSH, log in to the Cluster Virtual IP address as the root user:

Username: **`root`**

Password: **`<password>`**

Choose from one of the following options:

- If you can connect to the Cluster Virtual IP address, restore access to the QRadar user interface. For more information, see the *IBM Security QRadar SIEM Troubleshooting Guide*.
- If you cannot connect to the Cluster Virtual IP address, go to **Step 2**.

Repeat the following procedure for the primary and secondary HA host IP addresses:

Step 2 Using SSH, log in to the HA host as the root user:

Username: **`root`**

Password: **`<password>`**

Choose one of the following options:

- If you cannot connect to the primary or secondary HA host using SSH, ensure that your network and hardware configuration is operational. If your network and hardware configuration is operational and you cannot connect to the primary and secondary HA host, contact Customer Support for further assistance.
- If can connect to the primary and secondary HA host, identify the most recently Active HA host in your HA cluster, see **Identifying the Recently Active HA Host In Your HA Cluster**.

Identifying the Recently Active HA Host In Your HA Cluster

To identify the most recently Active host in your HA cluster:

Step 1 Using SSH, log in to the Primary HA Host as the root user:

Username: **root**

Password: **<password>**

Step 2 Display the HA cluster configuration by typing the following command:

cat /proc/drbd

The output may resemble the following:

```
version: 8.3.12 (api:88/proto:86-96)
GIT-hash: e2a8ef4656be026bbae540305fcb998a5991090f build by
dag@Build64R6, 2011-11-20 10:57:03
0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate C r
ns:513498760 nr:0 dw:303564200 dr:212968345 al:20474 bm:12829
lo:0 pe:0 ua:0 ap:0 ep:1 wo:d oos:0
```

Step 3 Review the following line in the output:

0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate

Choose from one of the following options:

- If the line does not display: **cs:Connected,** contact Customer Support to determine the most recently Active HA host in your cluster.
- If the line displays **ro:Primary/Secondary,** the Primary HA host is the Active system, go to **Step 5**.
- If the line displays **ro:Secondary/Primary,** the secondary HA host is the Active system, go to **Step 5**.
- If the line displays **ro:Secondary/Secondary,** go to **Step 4**.

Step 4 Review the following line in the output:

0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate

Choose one of the following options:

- If the line displays: **ds:< >/< >,** contact Customer Support to determine the most recently Active HA host in your HA cluster.
- If the line displays: **ds:< >/UpToDate,** the Secondary HA Host is the Active system, go to **Step 5**.
- If the line displays: **ds:UpToDate/< >,** the Primary HA Host is the Active system, go to **Step 5**.
- If the line displays: **ds:UpToDate/UpToDate,** contact Customer Support to determine the most recently Active HA host in your HA cluster.

Step 5 Contact Customer Support for assistance with restoring your Active HA host.

Offline Primary and Active Secondary

On the System and License Management window, if the primary HA host displays a status of Offline, set the primary HA host Online.

To set the primary HA host Online:

Step 1 Click the **Admin** tab.

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

Step 3 Click **System and License Management**.

Step 4 Select the primary HA host that you want to restore.

Step 5 From the **High Availability** menu, select **Set System Online**.

Step 6 On the System and License Management window, verify the status of the primary HA host. Choose from one of the following options:

- If the primary HA host displays a status of Active, you have restored the primary HA host.
- If the primary HA host displays a status of Offline, restore the primary HA host. For more information, see **Restoring a Failed Primary HA Host**.

A NOTICES AND TRADEMARKS

What's in this appendix:

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 *www.ibm.com/legal/copytrade.shtml*.

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

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

INDEX