IBM Security QRadar SIEM
Version 7.2.6

High Availability Guide

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

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to QRadar high-availability deployments v

Chapter 1. HA overview 1
Data consistency for HA 1
Real-time data synchronization 2
Post-failover data synchronization 2
HA clusters 2
Failovers 4
Primary HA host failure 4
Secondary HA host failure 4
Non-failover scenarios 4
HA failover event sequence 5
Network connectivity tests 5
Heartbeat ping tests 5
Primary disk failure 5
Manual failovers 6

Chapter 2. HA deployment planning 7
Firmware update 7
Appliance requirements 7
Software and virtual appliance requirements 8
System requirements for virtual appliances 8
IP addressing and subnets 10
Link bandwidth and latency 10
Data backup requirements 11
Offboard storage requirements for HA 11

Chapter 3. HA management 13
Status of HA hosts 13
Viewing HA cluster IP addresses 15
Creating an HA cluster 15
Disconnecting an HA cluster 18
Updating the `/etc/fstab` file 18
Editing an HA cluster 18
Setting an HA host offline 19
Setting an HA host online 19
Switching a primary HA host to active 19

Chapter 4. Recovery options for HA appliances 21
Notebook hyperterminal connections 21
Network connections 21
Recovering a secondary HA console or non-console 22
Recovering a failed primary HA host 23
Recovering a failed secondary HA host to IBM Security QRadar SIEM 7.1 24
Recovering a failed secondary HA host to IBM Security QRadar SIEM 7.1 (MR2) 25
Recovering a failed primary high-availability (HA) QFlow appliance 26
Recovering QRadar on a secondary high-availability HA console or non-console system 26
Recovering IBM Security QRadar on a failed primary HA console or non-console 27
Recovering a secondary HA host to a previous version or factory default 28

Chapter 5. Troubleshooting QRadar HA deployments 31
Restoring a failed secondary HA host 32
Restoring a failed primary HA host 32
Verifying the status of primary and secondary hosts 33

Setting the status of the primary HA host to online 33

Chapter 6. Disaster recovery in QRadar deployments 35
Primary QRadar Console and backup QRadar Console 35
Configuring the IP address on the backup console 36
Backup and recovery 36
Event and flow forwarding from a primary data center to another data center 36
Event and flow forwarding configuration 38
Load balancing of events and flows between two sites 39
Restoring configuration data from the primary to the secondary QRadar Console 39
Event and flow data redundancy 40

Notices 43
Trademarks 45
Privacy policy considerations 45

Introduction to QRadar high-availability deployments

Administrators can protect IBM® Security QRadar® data by implementing a high-availability (HA) solution.

Intended audience

QRadar SIEM administrators who are responsible for installing and deploying the product must know their corporate network infrastructure, the Linux operating system, and networking technologies.

Technical documentation

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

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

Contacting customer support

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

Statement of good security practices

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

Please Note:

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

Chapter 1. HA overview

If your hardware or network fails, IBM Security QRadar can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

To enable HA, QRadar connects a primary HA host with a secondary HA host to create an HA cluster.

If a primary HA host fails, then the secondary HA host maintains access to the same data as the primary by using data synchronization or shared external storage.

The secondary HA host inherits the license from the primary HA host. There is no need to apply a separate license to the secondary host.

For more information about using shared external storage with HA, for example iSCSI, Fibre Channel, or NFS, see the *IBM Security QRadar Offboard Storage Guide*.

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

Related concepts:

"HA clusters" on page 2
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

"Data consistency for HA"
When an HA failover occurs, IBM Security QRadar ensures the consistency of your data.

Data consistency for HA

When an HA failover occurs, IBM Security QRadar ensures the consistency of your data.

The type of storage that you use determines how HA data consistency is maintained. If you configure HA with external storage, data consistency is maintained by using a component such as an iSCSI or Fibre Channel external storage device. See "Offboard storage requirements for HA" on page 11.

If you do not use external storage devices, then QRadar HA maintains data consistency between a primary and secondary HA host by using Distributed Replicated Block Device.

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

Data synchronization occurs in the following situations in an HA environment:

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

Related concepts:

Chapter 1, "HA overview," on page 1
If your hardware or network fails, IBM Security QRadar can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

"Link bandwidth and latency" on page 10
To configure high-availability (HA), you must consider the bandwidth and latency between the primary and secondary HA hosts.

"Status of HA hosts" on page 13
You can review the status of the primary and secondary host in your high-availability (HA) cluster.

Real-time data synchronization

When 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.

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.

After synchronization is complete, the secondary HA host assumes a status of standby.

Depending on the size of the primary `/store` partition and performance, disk synchronization can take an extended time period. Ensure that the connection between the primary and secondary HA host has a minimum bandwidth of 1 Gbps.

Related concepts:

"Status of HA hosts" on page 13
You can review the status of the primary and secondary host in your high-availability (HA) cluster.

Post-failover data synchronization

Data that is collected by a primary high-availability (HA) host, up to the point of failover, is maintained virtually, in real time, by the secondary HA host.

When restored from a failover, the status of the primary HA host becomes offline. You must set the primary HA host to an online state before it can become the active host. Disk replication with the secondary HA host is enabled while the primary HA host remains offline.

When the primary HA host is restored, only the data that is collected by the secondary HA host in the intervening period is synchronized with the primary HA host. Therefore, post-failover disk synchronization is faster than initial disk synchronization, unless the disk on the primary HA host was replaced or reformatted when the host was manually repaired.

Related tasks:

"Setting an HA host online" on page 19
You can set the primary or secondary HA host to Online.

HA clusters

A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

Primary HA host

The primary HA host is any console or managed host in your IBM Security QRadar SIEM deployment that requires protection from data loss in the event of a failure.

When you create an HA cluster, the IP address of the primary HA host is automatically reassigned to a cluster virtual IP address. Therefore, you must assign an unused IP address to the primary HA host.

The primary HA host can act as a standby system for the secondary HA host. For example, if the primary HA host is repaired after a failover, the status changes to standby.

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 takes over all the responsibilities of the primary HA host.

Virtual IP address

When you create an HA cluster, the cluster virtual IP address takes the IP address of the primary HA host.

Configuring the cluster

Use the HA wizard to configure the primary host, secondary host, and cluster virtual IP address.

The following items are validated when you configure by using the HA wizard::

- the secondary HA host has a valid HA activation key.
- the secondary HA host is not part of another HA cluster
- the software versions on the primary and secondary HA hosts are the same
- if the primary HA host is configured with an external storage device, the secondary HA host is configured to access the same external storage device.
- the primary and secondary HA hosts support the same Device Support Module (DSM), scanner, and protocol RPMs.

Related concepts:

Chapter 1, “HA overview,” on page 1
If your hardware or network fails, IBM Security QRadar can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

“Primary HA host failure” on page 4
If the secondary high-availability (HA) host detects a primary failure, it automatically takes over the responsibilities of the primary HA host and becomes the active system.

“Status of HA hosts” on page 13
You can review the status of the primary and secondary host in your high-availability (HA) cluster.

“IP addressing and subnets” on page 10
To configure high-availability (HA), you must consider the subnet that is used by the secondary HA host and the virtual IP address.

Related tasks:

"Creating an HA cluster" on page 15
Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Failovers

When a primary or secondary high-availability (HA) host fails, IBM Security QRadar maintains data consistency.

The following scenarios cause failover:

- A power supply failure.
- A network failure that is detected by network connectivity tests.
- An operating system malfunction that delays or stops the heartbeat ping tests.
- A complete Redundant Array of Independent Disks (RAID) failure on the primary HA host.
- A manual failover.
- A management interface failure on the primary HA host.

Primary HA host failure

If the secondary high-availability (HA) host detects a primary failure, it automatically takes over the responsibilities of the primary HA host and becomes the active system.

When a primary HA host is recovered from a failover, it does not automatically take over the active status in the HA cluster. Instead, the secondary HA host remains the active system and the primary host acts as the standby system.

You must switch the primary back to the active status after successfully recovering from a primary failure.

Related concepts:

"HA clusters" on page 2
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

Related tasks:

"Switching a primary HA host to active" on page 19
You can set the primary high-availability (HA) host to be the active system.

Secondary HA host failure

If the primary high-availability (HA) host detects a secondary failure, it automatically assumes the responsibilities of the secondary HA host and becomes the active system.

If the primary HA host detects a secondary failure, it automatically assumes the responsibilities of the secondary HA host and becomes the active system.

Non-failover scenarios

HA failover does not occur when IBM Security QRadar detects software errors or disk capacity issues.

The following issues do not cause an automatic HA failover:

- If a QRadar process develops an error, stops functioning, or exits with an error.
- If a disk on your primary HA host reaches 95% capacity, QRadar data collection stops, but the primary HA host continues to function.

HA failover event sequence

IBM Security QRadar initiates a sequence of events when a primary high-availability (HA) host fails.

During failover, the secondary HA host assumes the responsibilities of the primary HA host. The following actions in sequence are completed in sequence:

1. If configured, external shared storage devices are detected and the file systems are mounted. For more information, see the IBM Security *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.

Network connectivity tests

To test network connectivity, the primary high-availability (HA) host automatically pings all existing managed hosts in your IBM Security 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 completes another network connectivity test with the managed hosts. If the test succeeds, the primary HA host completes a controlled failover to the secondary HA host. If the test fails, HA failover is not completed because the secondary HA host might also be experiencing network connectivity problems.

Related tasks:

"Creating an HA cluster" on page 15
Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Heartbeat ping tests

You can test the operation of the primary high-availability (HA) host by configuring the time interval of heartbeat ping tests.

If the secondary HA host does not receive a response from the primary HA host within a preconfigured time period, automatic failover to the secondary HA host is completed.

Related tasks:

"Creating an HA cluster" on page 15
Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Primary disk failure

If RAID completely fails and all disks are unavailable, the primary HA host completes a shutdown and fails over to the secondary HA host.

After a failover, the primary HA host assumes a status of **Failed**.

Related concepts:

"Status of HA hosts" on page 13
You can review the status of the primary and secondary host in your high-availability (HA) cluster.

Manual failovers

You can manually force a failover from a primary high-availability (HA) host to a secondary HA host.

Manually forcing a failover is useful for planned hardware maintenance on a console or managed host. Ensure the following before you conduct a manual failover:

- The primary and secondary HA hosts are synchronized.
- The secondary HA host has a status of standby.

To perform hardware maintenance on the primary HA host, set the primary system to offline to make the secondary HA host active. After the secondary host becomes active, you can shut down the primary host.

For hardware maintenance on the secondary HA host, set the secondary HA host to offline, and power off the secondary HA host.

For more information about manual failovers, see "Setting an HA host offline" on page 19.

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

Related tasks:

"Setting an HA host offline" on page 19
You can set the primary or secondary high-availability (HA) host to **Offline** from the **Active** or **Standby** state.

Chapter 2. HA deployment planning

Plan your high-availability deployment.

Before you implement high-availability (HA), review all the requirements to understand and prepare your IBM Security QRadar deployment.

Firmware update

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

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

Appliance requirements

Before you add a secondary host to your IBM Security QRadar SIEM Console, you must review the hardware configuration differences between your primary and secondary appliances.

Appliances that you order as primary and secondary HA pairs are matched to ensure compatibility. However, replacing an appliance or adding HA to an older Console with a different hardware configuration can lead to data replication issues. Data replication issues can occur when you replace end-of-life hardware or create primary and secondary HA pairs that have appliances from different manufacturers.

`/Store` partition requirements

- The file system of the `/store` partition must match between your primary and secondary host.

  Example: If the `/store` partition on the primary uses ext-3 as the file system, then your secondary must also use ext-3 for `/store`. A mismatch of the file system for the `/store` partition is not allowed.
- The size of the `/store` partition on the secondary must be equal to or larger than the `/store` partition of the primary.

For example, do not pair a primary host that uses a 3 TB `/store` partition to a secondary host that has a 2 TB `/store` partition.

Storage requirements

Follow these storage requirements when you replace an appliance:

- Ensure that the replacement appliance includes storage capacity that is equal to or greater than the original hardware you replace.
- Secondary replacement appliances can have larger storage capacity than the primary appliance. If so, partitions on the secondary are resized to match the storage capacity of the primary appliance when you configure the HA pair.

- Primary replacement appliances can have larger storage capacity than the secondary appliance. If so, partitions on the primary are resized to match the storage capacity of the secondary appliance when you configure the HA pair.
- If you replace both primary and secondary appliances, then the system resizes the storage partition that is based on the appliance with the smallest capacity.

Managed interfaces

- The primary host does not contain more physical interfaces than the secondary.

  If there is a failover, the network configuration of the primary is replicated to the secondary host. If the primary is configured with more interfaces, any additional interfaces cannot be replicated to the secondary during a failover.
- The secondary host must use the same management interface as the primary HA host.

  If the primary HA host uses eth0, for example, as the management interface, the secondary HA host must also use eth0.
- The management interface supports one cluster virtual IP address.
- TCP port 7789 must be open and allow communication between the primary and secondary for Distributed Replicated Block Device traffic.

  Distributed Replicated Block Device traffic is responsible for disk replication and is bidirectional between the primary and secondary host.
- You must ensure the QRadar software version is identical between the primary and secondary host before you pair a primary to a secondary appliance for the first time.

  If the QRadar version between your primary and secondary differ, you must patch either the primary or secondary appliance to ensure both appliances use the same software version.

  After the primary and secondary appliances are paired together, disk replication ensures that any additional software updates are also applied to the secondary.
- Ensure that the secondary host has a valid HA activation key.

Software and virtual appliance requirements

If you install IBM Security QRadar SIEM software on your own hardware or use virtual appliances, review the following requirements before you attempt to configure High-availability (HA).

System requirements for virtual appliances

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

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

Table 1. Requirements for virtual appliances

Requirement	Description
VMware client	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 For more information about VMWare clients, see the VMware website (www.vmware.com)

Table 1. Requirements for virtual appliances (continued)

Requirement	Description
Virtual disk size on QRadar VFlow Collector, QRadar Event Collector, QRadar Event Processor, QRadar Flow Processor, QRadar All-in-One, and QRadar Log Manager appliances	Minimum: 256 GB **Important:** For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
Virtual disk size for QRadar QFlow Collector appliances	Minimum: 70 GB
Virtual disk size for QRadar Risk Manager appliances	Suggested virtual disk size for implementation with up to 10000 configuration sources: 1 TB.
Virtual disk size for QRadar Vulnerability Manager processor appliances	50000 IP addresses - 500 GB 150000 IP addresses - 750 GB 300000 IP addresses - 1 TB
Virtual disk size for QRadar Vulnerability Manager scanner appliances	20000 IP addresses - 150 GB

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

Table 2. Minimum and optional memory requirements for QRadar virtual appliances

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

Table 3. Sample **CPU** *page settings*

Number of processors	Performance based on QRadar appliances
4	Log manager 3190: 2500 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 2500 events per second or less. All-in-One 3190: 25000 flows per minute or less, 500 events per second or less. Flow Processor 1790: 150,000 flows per minute. Dedicated Console 3190
8	Log manager 3190: 5000 events per second or less. Log manager Event Processor 1690, or SIEM Event Processor 1690: 5000 events per second or less. All-in-One 3190: 50000 flows per minute or less, 1000 events per second or less. Flow Processor 1790: 300,000 flows per minute.
12	All-in-One 3190: 100,000 flows per minute or less, 1000 events per second or less.
16	Log manager Event Processor 1690, or SIEM Event Processor 1690: 20,000 events per second or less. All-in-One 3190: 200,000 flows per minute or less, 5000 events per second or less.

IP addressing and subnets

To configure high-availability (HA), you must consider the subnet that is used by the secondary HA host and the virtual IP address.

Administrators must ensure that the following conditions are met:

- The secondary host is in the same subnet as the primary host.
- When the IP address of the primary host is reassigned as a cluster virtual IP, the new IP address that you assign must be in the same subnet.
- The secondary HA host that you want to add to the HA cluster is not a component in another HA cluster.

Related concepts:

"HA clusters" on page 2
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

Link bandwidth and latency

To configure high-availability (HA), you must consider the bandwidth and latency between the primary and secondary HA hosts.

If your HA cluster is using disk synchronization, the following conditions must be met:

- 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 increases with distance. If latency rises above 2 ms, then system performance is affected.

Related concepts:

"Data consistency for HA" on page 1
When an HA failover occurs, IBM Security QRadar ensures the consistency of your data.

Data backup requirements

There are items to consider for data backup before you configure hosts for High-availability (HA).

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 is removed from the deployment after a backup is completed, the secondary HA host displays a **Failed** status on the System and License Management window.

For more information about restoring backup archives in an HA environment, see the *IBM Security QRadar SIEM Administration Guide*

Offboard storage requirements for HA

You can implement high-availability (HA) when the IBM Security QRadar `/store` partition is mounted to an external storage solution, such as an iSCSI or Fibre Channel device.

If you implement an external storage solution, the data that is received by the primary HA host is automatically moved to the external device. It remains accessible for searching and reporting.

If a failover occurs, the `/store` partition on the secondary HA host is automatically mounted to the external device. On the external device, it continues to read and write to the data received by the primary HA host before the failover.

For more information about configuring shared external storage with HA, see the IBM Security QRadar *Offboard Storage Guide*

Administrators must review the following HA requirements before you implement an offboard storage device:

- The primary HA host must be configured to communicate with the external device. The data in the `/store` partition of the local disk must be moved to the external storage device.
- The secondary HA host must be configured to communicate with the external device. In doing so, when a primary HA host fails over, the secondary HA host can detect the external storage device.

- You must create an HA cluster only after the secondary HA host is configured to access the same external storage device.
- If you must reconfigure your external storage device or HA cluster settings, you must remove the HA cluster between the primary and secondary HA host. For more information, see *Disconnecting an HA cluster*.
- Ensure that there is at least a 1 Gbps connection between each HA host and your external device.

Important: During an upgrade to QRadar, you must reconfigure the external storage device connections to the hosts in your HA cluster. For more information, see the *Reconfiguring offboard storage during a QRadar upgrade technical note*.

Chapter 3. HA management

If you are required to tune, troubleshoot, or update your high-availability (HA) settings, use the System and License Management window on the IBM Security QRadar SIEM **Admin** tab.

Administrators can use the System and License management window to complete the following HA tasks:

- Monitor the state of an HA cluster.
- Force the manual failover of a primary HA host to complete maintenance on the primary host.
- Disconnect an HA cluster to alter the partitions of the primary and secondary HA hosts.
- Configure the ping test time period after which automatic failover to a secondary HA host occurs.
- Modify the HA cluster settings that are used to control network connectivity testing.

Status of HA hosts

You can review the status of the primary and secondary host in your high-availability (HA) cluster.

The following table describes the status of each host that is displayed in the System and License Management window:

Table 4. HA status descriptions

Status	Description
Active	Specifies that the host is the active system and that all services are running normally. The primary or secondary HA host can display the active status. **Note:** If the secondary HA host displays the active status, the primary HA host failed.
Standby	Specifies that the host is acting as the standby system. In the standby state, no services are running but data is synchronized if disk replication is enabled. If the primary or secondary HA host fails, the standby system automatically becomes the active system.
Failed	Specifies that the primary or secondary host failed. If the primary HA host displays Failed, the secondary HA host assumes the responsibilities of the primary HA host and displays the Active status. If the secondary HA host displays Failed, 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. If the network fails, you might need access to the physical appliance.

Table 4. HA status descriptions (continued)

Status	Description
Synchronizing	Specifies that data is synchronizing between hosts. **Note:** This status is displayed only when disk replication is enabled.
Online	Specifies that the host is online.
Offline	Specifies that an administrator manually set the HA host offline. Offline mode indicates a state that is typically used to complete appliance maintenance. When an appliance indicates a status of offline: Data replication is functioning between the active and offline HA hosts. Services that process events, flows, offenses, and heartbeat ping tests are stopped for the offline HA host. Failover cannot occur until the administrator sets the HA host online.
Restoring	Specifies that the host is restoring. For more information, see "Verifying the status of primary and secondary hosts" on page 33.
Needs License	Specifies that a license key is required for the HA cluster. In this state, no processes are running. For more information about applying a license key, see your *Administration Guide*.
Setting Offline	Specifies that an administrator is changing the status of an HA host to offline.
Setting Online	Specifies that an administrator is changing the status of an HA host to online
Needs Upgrade	Specifies that the secondary HA host requires a software upgrade. When the **Needs Upgrade** status is displayed, the primary remains active, but is not protected against failover. Disk replication of events and flows continues between the primary and the secondary HA hosts.
Upgrading	Specifies that the secondary HA host is being upgraded by the primary HA host. 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. After DSMs or protocols are installed and deployed on a Console, 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. Only a secondary HA host can display an Upgrading status.

Related concepts:

"Real-time data synchronization" on page 2
When 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.

"HA clusters" on page 2
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

"Primary disk failure" on page 5
If RAID completely fails and all disks are unavailable, the primary HA host completes a shutdown and fails over to the secondary HA host.

"Data consistency for HA" on page 1
When an HA failover occurs, IBM Security QRadar ensures the consistency of your data.

Related tasks:

"Verifying the status of primary and secondary hosts" on page 33
You must verify that the primary and secondary HA hosts are operational.

Viewing HA cluster IP addresses

You can display the IP addresses of all the components in your High-availability (HA) cluster.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Identify the QRadar primary console.
5. Hover your mouse over the **host name** field.

Creating an HA cluster

Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Before you begin

If a primary HA host has external storage configured, you must also configure the secondary HA host to use the same external storage options. For more information, see the QRadar *Offboard Storage Guide*.

About this task

If disk synchronization is enabled, it might take 24 hours or more for the data in the /store partition on the primary HA host /store partition to initially synchronize with the secondary HA host.

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.

In an HA deployment, the interfaces on both the primary and secondary HA hosts can become saturated. If performance is impacted, you can use a second pair of interfaces on the primary and secondary HA hosts to manage HA and data replication. Use a crossover cable to connect the interfaces.

Procedure

1. Click the **Admin** tab.
2. On the **navigation menu,** click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the host for which you want to configure HA.
5. From the **Actions** menu, select **Add HA Host** and click **OK**.
6. Read the introductory text. Click **Next**.
7. Type values for the parameters:

Option	Description
Primary Host IP address	A new primary HA host IP address. The new IP address replaces the previous IP address. The current IP address of the primary HA host becomes the Cluster Virtual IP address. The new primary HA host IP address must be on the same subnet as the virtual host IP address. For IPv6, if you selected **Yes** to auto-configure QRadar for IPv6 during the installation, enter the IP address that you recorded.
Secondary HA host IP address	The IP address of the secondary HA host. The secondary HA host must be on the same subnet as the primary HA host.
Enter the root password of the host	The root password for the secondary HA host. The password must not include special characters.
Confirm the root password of the host	The root password for the secondary HA host again for confirmation.

8. To configure advanced parameters, click the arrow beside **Show Advanced Options** and type values for the parameters.

Option	Description
Heartbeat Interval (seconds)	The time, in seconds, that you want to elapse between heartbeat pings. The default is 10 seconds. For more information about heartbeat pings, see “Heartbeat ping tests” on page 5.
Heartbeat Timeout (seconds)	The time, in seconds, that you want to elapse before the primary HA host is considered unavailable if no heartbeat is detected. The default is 30 seconds.

Option	Description
Network Connectivity Test List peer IP addresses (comma delimited)	The IP addresses of the hosts that you want the secondary HA host to ping. The default is to ping all other managed hosts in the QRadar deployment. For more information about network connectivity testing, see "Network connectivity tests" on page 5.
Disk Synchronization Rate (MB/s)	The disk synchronization rate. The default is 100 MB/s.
Disable Disk Replication	This option is displayed only when you are configuring an HA cluster by using a managed host.
Configure Crossover Cable	Crossover cables allow QRadar to isolate the replication traffic from all other QRadar traffic, such as events, flows, and queries.
Crossover Interface	Select the interfaces that you want to connect to the primary HA host. Only interfaces with an active link appear in the list.
Crossover Advanced Options	Select **Show Crossover Advanced Options** to enter, edit, or view the property values.

9. Click **Next**, and then click **Finish**.

   Important: When an HA cluster is configured, you can display the IP addresses that are used in the HA cluster. Hover your mouse over the **Host Name** field on the System and License Management window.

Related concepts:

"HA clusters" on page 2
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

"Network connectivity tests" on page 5
To test network connectivity, the primary high-availability (HA) host automatically pings all existing managed hosts in your IBM Security QRadar deployment.

"Heartbeat ping tests" on page 5
You can test the operation of the primary high-availability (HA) host by configuring the time interval of heartbeat ping tests.

Related tasks:

"Recovering a secondary HA console or non-console" on page 22
You can install or recover a secondary high-availability (HA) IBM Security QRadar or non-console (managed host) appliance.

"Recovering IBM Security QRadar on a failed primary HA console or non-console" on page 27
You can recover IBM Security QRadar console or non-console (managed host) software on your failed primary HA host.

Disconnecting an HA cluster

By disconnecting an HA cluster, the data on your primary HA console or managed host is not protected against network or hardware failure.

Before you begin

If you migrated the /store file system to a Fibre Channel device, you must modify the /etc/fstab file before you disconnect the HA cluster. For more information, see "Updating the /etc/fstab file."

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the HA host that you want to remove.
5. From the toolbar, select **High Availability** > **Remove HA Host**.
6. Click **OK**.

Note: When you remove an HA host from a cluster, the host restarts.

Updating the /etc/fstab file

Before you disconnect a Fibre Channel HA cluster, you must modify the /store and /store/tmp mount information in the /etc/fstab file.

About this task

You must update the /etc/fstab file on the primary HA host and the secondary HA host.

Procedure

1. Use SSH to log in to your QRadar host as the root user:
2. Modify the etc/fstab file.
   a. Locate the existing mount information for the /store and /store/tmp file systems.
   b. Remove the **noauto** option for the /store and /store/tmp file systems.
3. Save and close the file.

What to do next

Disconnecting an HA cluster.

Editing an HA cluster

You can edit the advanced options for your HA cluster.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the row for the HA cluster that you want to edit.

5. From the toolbar, select **High Availability** > **Edit HA Host**.
6. Edit the parameters in the table in the advanced options section.
7. Click **Next**.
8. Review the information.
9. Click **Finish**.

Setting an HA host offline

You can set the primary or secondary high-availability (HA) host to **Offline** from the **Active** or **Standby** state.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the HA host that you want to set to offline.
5. From the toolbar, select **High Availability** > **Set System Offline** .

Related concepts:

"Manual failovers" on page 6
You can manually force a failover from a primary high-availability (HA) host to a secondary HA host.

Setting an HA host online

You can set the primary or secondary HA host to Online.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the offline HA host that you want to set to Online.
5. From the toolbar, select **High Availability** > **Set System Online**.

What to do next

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

- If the primary HA host displays a status of **Active**, HA host is restored.
- If you experience a problem, restore the primary or secondary HA host. For more information, see *Restoring a failed secondary HA host* or *Restoring a failed primary HA host*.

Related concepts:

"Post-failover data synchronization" on page 2
Data that is collected by a primary high-availability (HA) host, up to the point of failover, is maintained virtually, in real time, by the secondary HA host.

Switching a primary HA host to active

You can set the primary high-availability (HA) host to be the active system.

Before you begin

The primary HA host must be the standby system and the secondary HA host must be the active system.

About this task

If your primary host is recovered from a failure, it is automatically assigned as the standby system in your HA cluster. You must manually switch the secondary HA host to be offline to make the primary HA host active.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. In the System and License Management window, select the **secondary HA host**.
5. From the toolbar, select **High Availability** > **Set System Offline**.

   Note: Your IBM Security QRadar SIEM user interface might be inaccessible during this time.

What to do next

When you can access the System and License Management window, check the **status** column. Ensure that the primary HA host is the active system and the secondary HA host is the standby system.

Related concepts:

"Primary HA host failure" on page 4
If the secondary high-availability (HA) host detects a primary failure, it automatically takes over the responsibilities of the primary HA host and becomes the active system.

Chapter 4. Recovery options for HA appliances

You can reinstall or recover IBM Security QRadar high-availability (HA) appliances.

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

Notebook hyperterminal connections

During the recovery of a IBM Security QRadar appliance, you can use a notebook to monitor the progress of the installation.

If you use HyperTerminal to monitor a QRadar reinstallation or recovery, choose from the connection parameters that are listed in the following table.

Table 5. Hyper terminal connection parameters

Parameter	Description
Connect Using	Select the appropriate COM port of the serial connector.
Bits per second	Type 9600
Stop Bits	Type 1
Data bits	Type 8
Type 8	Type None

Related tasks:

"Recovering a secondary HA console or non-console" on page 22
You can install or recover a secondary high-availability (HA) IBM Security QRadar or non-console (managed host) appliance.

Network connections

During the recovery or reinstallation of a IBM Security QRadar appliance, you can specify the network connection settings.

Use the information in the following table when you recover or reinstall a QRadar appliance:

Table 6. QRadar network setting parameters

Parameter	Description
Hostname	Type a fully qualified domain name as the system host name.
IP Address	Type the IP address of the system. **Note:** If you are recovering an HA appliance, the IP address is the primary HA host IP address. You can identify the IP address in the System and License Management window.
Network Mask	Type the network mask address for the system.

Table 6. QRadar network setting parameters (continued)

Parameter	Description
Gateway	**Optional:** Type the **Public IP address** of the server. The **Public IP address** is a secondary IP address that is used to access the server. Access is usually from a different network or the Internet, and is managed by your network administrator. The **Public IP address** is often configured by using Network Address Translation (NAT) services or firewall settings on your network.
Email Server	Type the email server. If you do not have an email server, type `localhost` in this field.

Recovering a secondary HA console or non-console

You can install or recover a secondary high-availability (HA) IBM Security QRadar or non-console (managed host) appliance.

Before you begin

To recover a primary or secondary console or non-console HA console or reinstall QRadar software, you must have a valid activation key.

The activation key is a 24-digit, 4-part, alphanumeric value. You can find the activation key:

- Printed on a sticker and physically placed on your console.
- Included with the packing slip. All consoles are listed along with their associated keys.

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

The build version of the primary HA host must be the same as the QRadar build version installed on the secondary HA host.

The secondary or primary HA host must be patched to the correct build version before you configure an HA cluster.

Procedure

1. Prepare your appliance.
   a. Install all necessary hardware.
   b. Connect a notebook to the serial port on the rear of the appliance, or connect a keyboard and monitor to their respective ports.

      For more information on your QRadar appliance or appliance ports, see the *IBM Security QRadar Hardware Guide*.
   c. Turn on the system and log in as **Username:** `root`

      Note: The user name is case-sensitive.
   d. Press Enter.
   e. Press the Spacebar to advance each window then type yes to accept the agreement and press **Enter**.

f. Type your activation key and press Enter.

2. Follow the instructions in the wizard.
3. Configure the QRadar network settings.
4. Select **Next** and press Enter.

   Note: If you are changing network settings with `qchange_netsetup`, select **Finish** and press Enter. For more information about changing network settings, see the *IBM Security QRadar SIEM Installation Guide* or the *IBM Security QRadar Log Manager Installation Guide*.
5. Configure the QRadar root password:
   a. Type your password, then select **Next** and press Enter.
   b. Retype your new password. Select **Finish** and press Enter.

      Note: This process can take several minutes.
   c. Press Enter to select OK.
6. Log in to the QRadar user interface.

What to do next

Configure the HA Cluster.

Related concepts:

"Notebook hyperterminal connections" on page 21
During the recovery of a IBM Security QRadar appliance, you can use a notebook to monitor the progress of the installation.

Related tasks:

"Creating an HA cluster" on page 15
Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Recovering a failed primary HA host

You can recover a failed primary high-availability (HA) IBM Security QRadar host.

Before you begin

If you need to reinstall QRadar on a failed primary high-availability (HA) host, you must consider the build version of the secondary HA host.

To recover a primary or secondary console or non-console HA console or reinstall QRadar software, you must have a valid activation key.

The activation key is a 24-digit, 4-part, alphanumeric value. You can find the activation key:

- Printed on a sticker and physically placed on your console.
- Included with the packing slip. All consoles are listed along with their associated keys.

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

The build version of the primary HA host must be the same as the QRadar build version installed on the secondary HA host.

The secondary or primary HA host must be patched to the correct build version before you configure an HA cluster.

Procedure

1. Install all necessary hardware.
2. Choose one of the following options:
   - Connect a notebook to the serial port on the rear of the appliance. For more information, see "Notebook hyperterminal connections" on page 21.
   - Connect a keyboard and monitor to their respective ports.
3. Turn on the system and login: **Username:** `root`
4. Press Enter.
5. Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
6. Type your activation key and press Enter.
7. Select **HA Recovery Setup** Select **Next** and press Enter.
8. Follow the instructions in the wizard.
9. Configure the QRadar network settings.
10. Select **Next** and press Enter.
11. Configure the QRadar root password.
12. Log in to the QRadar user interface.
13. Restore the failed primary HA host. For more information, see "Verifying the status of primary and secondary hosts" on page 33.

Recovering a failed secondary HA host to IBM Security QRadar SIEM 7.1

You can recover a failed secondary high-availability (HA) host to IBM Security QRadar SIEM v7.1.

About this task

When you recover a failed secondary HA host that used a previous QRadar version, you can install QRadar 7.1 from an updated recovery partition.

The installer repartitions and reformats the hard disk, installs the Operating System, then reinstalls QRadar. Wait for the flatten process to complete. This process can take several minutes.

For more information on installing your secondary HA host, see the *IBM Security QRadar Installation Guide* or the *IBM Security QRadar Log Manager Administration Guide*.

Procedure

1. Using SSH, log in to the secondary HA host as the root user:
   a. **Username:**`root`
   b. **Password:**`<password>`
2. Obtain the QRadar software from the following location: https://www.ibm.com/support
3. Copy the QRadar 7.1 ISO to the secondary HA host by typing the following command: **`scp <iso file name> root@<ip_address>:/root`**

Important: If you are installing QRadar 7.0 and above, Step 4 through Step 5 are not necessary. The recovery script is placed in `/opt/qradar/bin` during the installation.

4. Mount the ISO by typing the following command: **mount -o loop <iso_file_name> /media/cdrom/**
5. Copy the recovery script into the root directory by typing the following command: **cp /media/cdrom/post/recovery.py /root**
6. Unmount the ISO by typing the following command: **umount /media/cdrom/**
7. If the host is a non-console, to stop the **IPTables** service to allow secure copy (SCP), type the following command:

   service iptables stop
8. Start the extracted recovery script by typing the following command: **./recovery.py -r --default --reboot <iso_file_name>**
9. When prompted, press Enter to restart the appliance.
10. When prompted, type `flatten` and press Enter.
11. When the installation completes, type `SETUP` and log in to the system as the root user.

Recovering a failed secondary HA host to IBM Security QRadar SIEM 7.1 (MR2)

When you recover a failed secondary high-availability (HA) host that used a previous IBM Security QRadar SIEM version, you can install QRadar 7.1 from an updated recovery partition.

Procedure

1. Using SSH, log in to the secondary HA host as the root user:
   a. **Username:**`root`
   b. **Password:**`<password>`
2. Obtain the QRadar software from the following location: https://www.ibm.com/support
3. Copy the QRadar 7.1 ISO to the secondary HA host by typing the following command: **scp <iso file name> root@<ip_address>:/root**
4. If the host is a non-console, to stop the **IPTables** service to allow secure copy (SCP), type the following command.

   service iptables stop
5. Start the extracted recovery script by typing the following command: **./recovery.py -r --default --reboot <iso_file_name>**
6. When prompted, press Enter to restart the appliance.
7. When prompted, type `flatten` and press Enter.

Results

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

Recovering a failed primary high-availability (HA) QFlow appliance

You can recover a failed primary high-availability (HA) IBM Security QRadar QFlow Collector.

Procedure

1. Install all necessary hardware.
2. Choose one of the following options:
   - Connect a notebook to the serial port on the rear of the appliance. For more information, see "Notebook hyperterminal connections" on page 21.
   - Connect a keyboard and monitor to their respective ports.
3. Turn on the system and login: **Username:** `root`
4. Press Enter.
5. Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
6. Type your activation key and press Enter.
7. Select **HA Recovery Setup**. Select **Next** and press Enter.
8. Select your time zone continent or area. Select **Next** and press Enter.
9. Select your time zone region. Select **Next** and press Enter.
10. Select **IPv4**. Select **Next** and press Enter.

    Note: Each interface with a physical link is denoted with a plus (+) symbol.
11. Select the **management interface**. Select **Next** and press Enter.
12. Type the **Cluster Virtual IP address**, then select **Next** and press Enter. For more information, see "Viewing HA cluster IP addresses" on page 15.
13. Configure the QRadar network settings. .
14. Select **Next** and press Enter.
15. Configure the QRadar root password.
16. Log in to the QRadar user interface.
17. Restore the failed primary HA host. For more information about restoring a failed primary HA host, see "Verifying the status of primary and secondary hosts" on page 33.

Recovering QRadar on a secondary high-availability HA console or non-console system

You can install or recover QRadar Console or non-console (managed host) software on your secondary high-availability (HA) system.

Before you begin

These instructions are applicable to the installation or recovery of a QRadar Console and non-console. You must choose different options according to the appliance you are installing or recovering.

Ensure that you have a QRadar activation key. For more information, see QRadar activation keys.

Procedure

1. Install the necessary hardware.

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

   Note: For instructions on how to install and configure the Red Hat Enterprise Linux operating system, see the *IBM Security QRadar Installation Guide*.
3. Log in as root.
4. Create the `/media/cdrom` directory by typing the following command: `mkdir /media/cdrom`
5. Obtain the QRadar software from the following location: https://www.ibm.com/support
6. Mount the QRadar ISO by typing the following command:`mount -o loop <path to the QRadar ISO> /media/cdrom`
7. Begin the installation by typing the following command: `/media/cdrom/setup`
8. Press the Spacebar to advance each window then type **yes** to accept the agreement and press Enter.
9. Type your activation key and press Enter.
10. Follow the instructions in the wizard.
11. Configure the QRadar network settings.
12. Select **Next** and press Enter.

    Note: If you are changing network settings by using **`qchange_netsetup`**, select **Finish** and press Enter. For more information, see the *IBM Security QRadar Installation Guide*.
13. Configure the QRadar root password.
14. Log in to the QRadar user interface.

What to do next

Configure the HA cluster.

Recovering IBM Security QRadar on a failed primary HA console or non-console

You can recover IBM Security QRadar console or non-console (managed host) software on your failed primary HA host.

Before you begin

These instructions are applicable to the installation or recovery of QRadar on a primary console and non-console. You must choose different options according to the appliance you are installing or recovering.

Ensure that you have a QRadar activation key. For more information, see QRadar activation keys.

Procedure

1. Install the necessary hardware.
2. Obtain the Red Hat Enterprise Linux operating system and install it on your hardware.

   Note: For instructions on how to install and configure the Red Hat Enterprise Linux operating system, see the *IBM Security QRadar Installation Guide*.

3. Log in as root.
4. Create the `/media/cdrom` directory by typing the following command: `mkdir /media/cdrom`
5. Obtain the QRadar software from the following location: https://www.ibm.com/support
6. Mount the QRadar ISO by typing the following command: `mount -o loop <path to the QRadar ISO> /media/cdrom`
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.
8. Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
9. Type your activation key and press Enter.
10. Follow the instructions in the wizard.
11. Configure the QRadar network settings.
12. Select **Next** and press Enter.
13. Configure the QRadar root password.
14. Log in to QRadar.

What to do next

Restore the failed primary HA host. See "Verifying the status of primary and secondary hosts" on page 33.

Related tasks:

"Creating an HA cluster" on page 15
Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using IBM Security QRadar creates an HA cluster.

Recovering a secondary HA host to a previous version or factory default

You can recover an IBM Security QRadar secondary high-availability (HA) host to a previous version or factory default.

About this task

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

Procedure

1. Using SSH, log in to the Console as the root user.
2. Using SmartCloud Provisioning, copy the `recovery.py` script from the Console to the failed secondary HA host.

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

3. Obtain the QRadar ISO from the following location: https://www.ibm.com./support
4. Use secure copy (SCP) to copy the ISO file to the target QRadar host.
   `scp <iso_file_name> root@<TargetIP_address>:/root`
5. Using SSH, log in to the secondary HA host.
6. Type the following commands:
   ```
   chmod 755 recovery.py
   ./recovery.py -r --default --reboot <iso_file_name>
   ```
7. Press Enter when prompted to restart the system.
8. When prompted, type `flatten` and press Enter.

Results

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. After the process is complete, the normal installation process continues.

Chapter 5. Troubleshooting QRadar HA deployments

Use the status of the HA hosts in the System and License Management window to help you troubleshoot.

Status combinations and possible resolutions

The following table describes the possible status settings for primary and secondary HA hosts. Each status combination requires a different troubleshooting approach.

Table 7. System and license management window host statuses.

Primary HA host status	Secondary HA host status	Possible action
Active	Failed or Unknown	Ensure that the secondary host is on, and that you can log on to it as a root user by using SSH. If you can connect, see "Restoring a failed secondary HA host" on page 32.
Failed or Unknown	Active	Ensure that the primary host is on, and that you can log on to it as a root user by using SSH. If you can connect, see "Restoring a failed primary HA host" on page 32.
Unknown	Unknown	If you cannot connect to the primary or secondary HA host by using SSH, ensure that your network and hardware configuration is operational.
Offline	Active	To set the primary host online, see Set the primary HA host online.

Identifying active hosts

You can identify the most recent active host in your HA cluster by using SSH.

1. To display the HA cluster configuration, type the following command:
   ```
   cat /proc/drbd
   ```
2. Review the following line: in the output:
   ```
   0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate
   ```
   - If the line does not display the following text, `cs:Connected`, determine the most recent active HA host in the HA cluster.
   - If the output displays the following text, `Secondary/Primary`, the secondary HA Host is the active system.
   - If the output displays the following text, `ro:Primary/Secondary`, the primary HA Host is the active system.
3. If the line displays `ro:Secondary/Secondary`, review the following line in the output:
   ```
   0: cs:Connected ro:Secondary/Secondary
   ```

- If the output displays the following text, `ds:< >/UpToDate`, the secondary HA Host is the active system.
- If the output displays the following text, `ds:UpToDate/< >`, the primary HA Host is the active system.
- If the output displays the following text, `ds:< >/< >`, determine the most recent active HA host in your HA cluster.
- If the output displays the following text, `ds:UpToDate/UpToDate`, determine the most recent active HA host in your HA cluster.

Restoring a failed secondary HA host

You can restore a failed secondary HA host.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.
4. Select the secondary HA host that you want to restore.
5. From the **High Availability** menu, click **Restore System**.
6. If the secondary HA host displays a status of **Failed** or **Unknown** in the System and License Management window, use SSH to log in to the secondary HA host as the root user to ensure that the host is operational.
7. Restart the secondary HA host by typing `reboot`.
8. After the system is restarted, if the secondary HA host displays a status of **Failed** or **Unknown**, from the **High Availability** menu, click **Restore System**.

Related tasks:

"Verifying the status of primary and secondary hosts" on page 33
You must verify that the primary and secondary HA hosts are operational.

Restoring a failed primary HA host

You can restore a failed primary HA host.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.
4. Select the primary HA host that you want to restore.
5. From the **High Availability** menu, click **Restore System**.
6. Verify the status of the primary HA host.
7. If the primary HA host displays a status of **Offline**, in the System and License Management window, click **High Availability** > **Set System Online**.
8. If the primary HA host displays a status of **Failed** or **Unknown** in the System and License Management window, use SSH to log in to the primary HA host as the root user to ensure that the host is operational.
9. Restart the primary HA host by typing the following command: **reboot**

Related tasks:

"Setting the status of the primary HA host to online" on page 33
If the primary HA host displays a status of offline, you can reset the status to online.

Verifying the status of primary and secondary hosts

You must verify that the primary and secondary HA hosts are operational.

Procedure

1. Identify whether the primary HA host was configured as a console or managed host.
2. If the primary HA host is configured as a console, use SSH to log in to the Cluster Virtual IP address as the root user:
   - If you can connect to the Cluster Virtual IP address, restore access to the QRadar. For more information, see the *IBM Security QRadar SIEM Troubleshooting Guide*.
   - If you cannot connect to the Cluster Virtual IP address, use SSH to log in to the secondary HA host as the root user to ensure that it is operational.
3. If your secondary host is configured as a managed host, use SSH to log in to the secondary HA host as the root user.
   - If you cannot connect to the primary or secondary HA host by using SSH, ensure that your network and hardware configuration is operational.
   - If you can connect to the primary and secondary HA host, identify the most recently active HA host in your HA cluster.

Related concepts:

"Status of HA hosts" on page 13
You can review the status of the primary and secondary host in your high-availability (HA) cluster.

Related tasks:

"Verifying the status of primary and secondary hosts"
You must verify that the primary and secondary HA hosts are operational.

Setting the status of the primary HA host to online

If the primary HA host displays a status of offline, you can reset the status to online.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.
4. Select the primary HA host that you want to restore.
5. In the System and License Management window, if the primary HA host displays a status of **Offline**, your must restore the primary HA host.

Related tasks:

"Restoring a failed primary HA host" on page 32
You can restore a failed primary HA host.

Chapter 6. Disaster recovery in QRadar deployments

Implement disaster recovery (DR) to safeguard your IBM Security QRadar configurations and data by mirroring your data to another identical QRadar system. Disaster recovery is possible when you have two identical QRadar systems in separate geographic environments that are a mirror of each other, and data is collected at both sites.

Enable disaster recovery (DR) when you forward live data, for example, flows and events from a primary QRadar system, to a parallel system at another site. Forwarding data uses *off-site forwarding*, which is set up on both the primary and secondary deployments. You can set up disaster recovery with deployments that are in different geographical locations.

Choose one of the following disaster recovery deployment scenarios:

Primary QRadar Console and backup console
A hardware failure solution, where the backup console is a copy of the primary server, with the same configuration but stays powered off. Only one console is operational at any one time. If the primary console fails, you manually turn the power on the backup console, apply the primary configuration backup, and use the IP address from the primary console. After you restore the primary server and before you turn it on, you manually turn off the backup server. If the system is down for a long time, apply the backup console configuration backup to the primary server.

Event and flow forwarding
Events and flows are forwarded from a primary site to a secondary site. Identical architectures in two separate data centers are required.

Distributing the same events and flows to the primary and secondary sites
Distribute the same event and flow data to two live sites by using a load balancer or other method to deliver the same data to mirrored appliances. Each site has a record of the log data that is sent.

Primary QRadar Console and backup QRadar Console

When the primary QRadar Console fails and you want the backup QRadar Console to take up the role of the primary, you manually turn the power on the backup console, apply the configuration backup and the IP address from the primary. Use a similar switchover method for other appliances such as a QRadar QFlow Collector or an Event Collector, where each appliance has a cold backup or spare that is an identical appliance.

The backup console takes over the primary QRadar Console role from the time of activation, and does not store past events, flow, or offenses from the original primary QRadar Console. Use this type of deployment for your appliances, to minimize downtime, when there is a hardware failure.

If the primary fails, take the following steps to set up the backup console as the primary QRadar Console:

1. Power on the backup console.
2. Add the IP address from the primary console.

3. Restore configuration backup data from the primary console to the backup console.

The backup console functions as the primary console until the primary console is brought back online. Ensure that both servers are not online at the same time.

Configuring the IP address on the backup console

When the primary QRadar Console fails, you configure the secondary backup console to take on the primary console role. Add the IP address of the failed QRadar Console to the backup console so that your QRadar system continues to function.

Before you begin

Power on the backup console.

Procedure

1. Use SSH to log in to as the root user.
2. To configure the IP address on the backup console, follow these steps:
   a. Type the following command:
      ```
      qchange_netsetup
      ```
   b. Follow the instructions in the wizard to enter the configuration parameters.
      After the requested changes are processed, the QRadar system automatically shuts down and restarts.

Backup and recovery

Back up your IBM Security QRadar configuration information and data so that you can recover from a system failure or data loss.

Use the backup and recovery that is built-in to QRadar to back up your data. However, you must restore the data manually. By default, QRadar creates a daily backup archive of your configuration information at midnight. The backup archive includes configuration information, generated data, or both from the previous day.

You can create the following types of backup:

- Configuration backups, which include system configuration data, for example, assets and log sources in your QRadar deployment.
- Data backups, which include information that is generated by a working QRadar deployment such as log information or event dates.

For more information about backing up and recovering your data, see the *IBM Security QRadar SIEM Administration Guide*.

Event and flow forwarding from a primary data center to another data center

To ensure that there is a redundant data store for events, flows, offenses, and that there is an identical architecture in two separate data centers, forward event and flow data from site 1 to site 2.

This scenario is dependent upon site 1 remaining active. If site 1 fails, data is not transmitted to Site 2, but the data is current up to the time of failure. In the case of

failure at site 1, you implement disaster recovery (DR), by manually changing IP addresses and use a backup and restore to fail over from site 1 to site 2, and to switch to site 2 for all QRadar hosts.

The following list describes the setup for event and flow forwarding from the primary site to the secondary site:

- There is an identical distributed architecture in two separate data centers, which includes a primary data center and a secondary data center.
- The primary QRadar Console is active and collecting all events and flows from log sources and is generating correlated offenses.
- You configure off-site targets on the primary QRadar Console to enable forwarding of event and flow data from the primary data center to the event and flow processors in another data center.

  Fast path: Use routing rules instead of off-site targets because the setup is easier.
- Periodically, use the content management tool to update content from the primary QRadar Console to the secondary QRadar Console.

For more information about forwarding destinations and routing rules, see the *IBM Security QRadar SIEM Administration Guide*.

In the case of a failure at site 1, you can use a high-availability (HA) deployment to trigger an automatic failover to site 2. The secondary HA host on site 2 takes over the role of the primary HA host on site 1. Site 2 continues to collect, store, and process event and flow data. Secondary HA hosts that are in a standby state don't have services that are running but data is synchronized if disk replication is enabled. For more information about HA deployment planning, see Chapter 2, “HA deployment planning,” on page 7.

Note: You can use a load balancer to divide events, and split flows such as NetFlow, J-Flow, and sFlow but you can't use a load balancer to split QFlows. Use external technologies such as a regenerative tap to divide QFlow and send to the backup site.

The following diagram shows how site 2 is used as a redundant data store for site 1. Event and flow data are forwarded from site 1 to site 2.

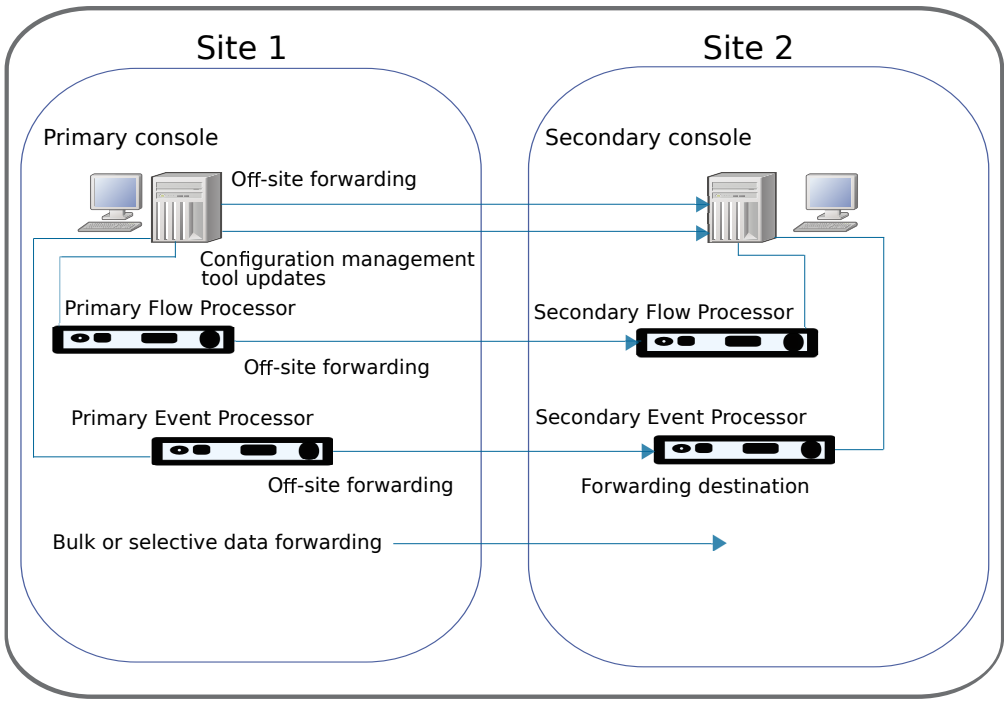

Figure 1. Event and flow forwarding from site 1 to site 2 for disaster recovery

Event and flow forwarding configuration

For data redundancy, configure IBM Security QRadar systems to forward data from one site to a backup site.

The target system that receives the data from QRadar is known as a *forwarding destination*. QRadar systems ensure that all forwarded data is unaltered. Newer versions of QRadar systems can receive data from earlier versions of QRadar systems. However, earlier versions cannot receive data from later versions. To avoid compatibility issues, upgrade all receivers before you upgrade QRadar systems that send data. Follow these steps to set up forwarding:

1. Configure one or more forwarding destinations.

   A forwarding destination is the target system that receives the event and flow data from the IBM Security QRadar primary console. You must add forwarding destinations before you can configure bulk or selective data forwarding. For more information about forwarding destinations, see the *IBM Security QRadar SIEM Administration Guide*.

2. Configure routing rules, custom rules, or both.

   After you add one or more forwarding destinations for your event and flow data, you can create filter-based routing rules to forward large quantities of data. For more information about routing rules, see the *IBM Security QRadar SIEM Administration Guide*.

3. Configure data exports, imports, and updates.

   You use the content management tool to move data from your primary QRadar Console to the QRadar secondary console. Export security and configuration content from IBM Security QRadar into an external, portable format. For more information about using the content management tool to transfer data, see the *IBM Security QRadar SIEM Administration Guide*.

Load balancing of events and flows between two sites

When you are running two live IBM Security QRadar deployments at both a primary and secondary site, you send event and flow data to both sites. Each site has a record of the log data that is sent. Use the content management tool to keep the data synchronized between the deployments

The following diagram shows two live sites, where data from each site is replicated to the other site.

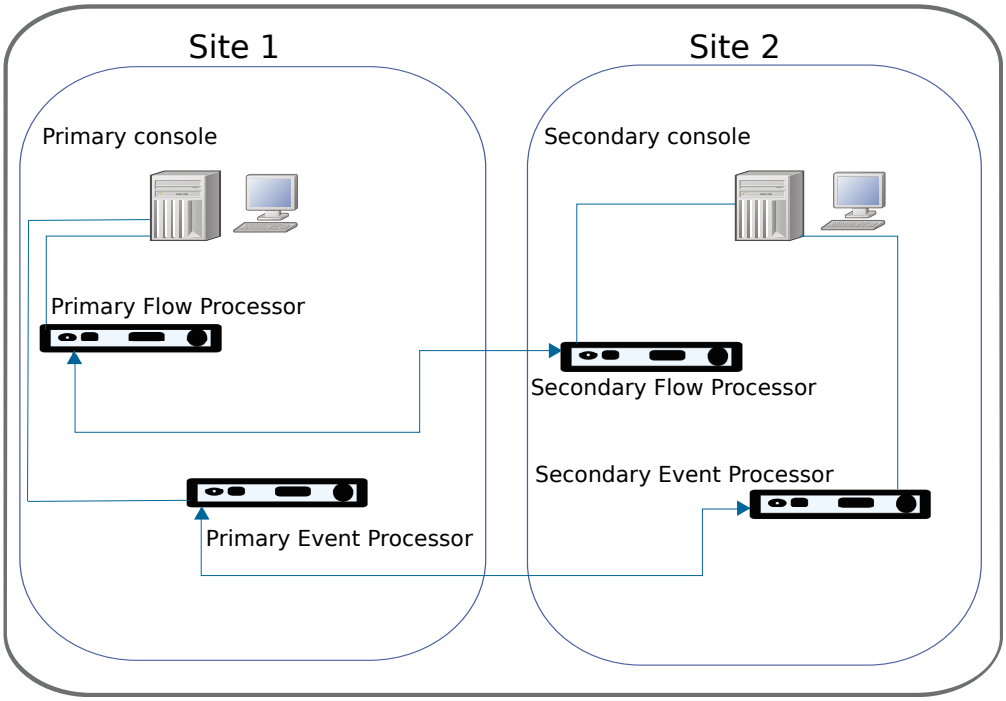

Figure 2. Load balancing of events and flows between two sites

Related concepts:

"Event and flow data redundancy" on page 40
Send the same events and flows to separate data centers or geographically separate sites and enable data redundancy by using a load balancer or other method to deliver the same data to mirrored appliances.

Restoring configuration data from the primary to the secondary QRadar Console

After you set up the secondary QRadar Console as the destination for the logs, you either add or import a backup archive from the primary QRadar Console. You can restore a backup archive that is created on another QRadar host. Log in to the secondary QRadar Console and do a full restore of the primary console backup archive to the secondary QRadar Console.

Before you begin

You must have a data backup from your primary console to complete this task.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Backup and Recovery** icon.
4. In the **Upload Archive** field, click **Browse**.
5. Locate and select the archive file that you want to upload.

   Tip: If the QRadar backup archive file is in the `/store/backupHost/inbound` directory on the console server, the backup archive file is automatically imported.

   The archive file must have a `.tgz` extension.
6. Click **Open**.
7. Click **Upload**.
8. Select the archive that you uploaded and click **Restore**.

   When the restore is finished, the secondary QRadar Console becomes the primary console.

Event and flow data redundancy

Send the same events and flows to separate data centers or geographically separate sites and enable data redundancy by using a load balancer or other method to deliver the same data to mirrored appliances.

Configure the distribution of log and flow sources for data redundancy:

- Send log source data to the Event Processor on the second site.
- Send flow source data to the Flow Processor on the second site.

  For more information about configuring log sources, see the *IBM Security QRadar Log Sources Configuration Guide*.

  For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.

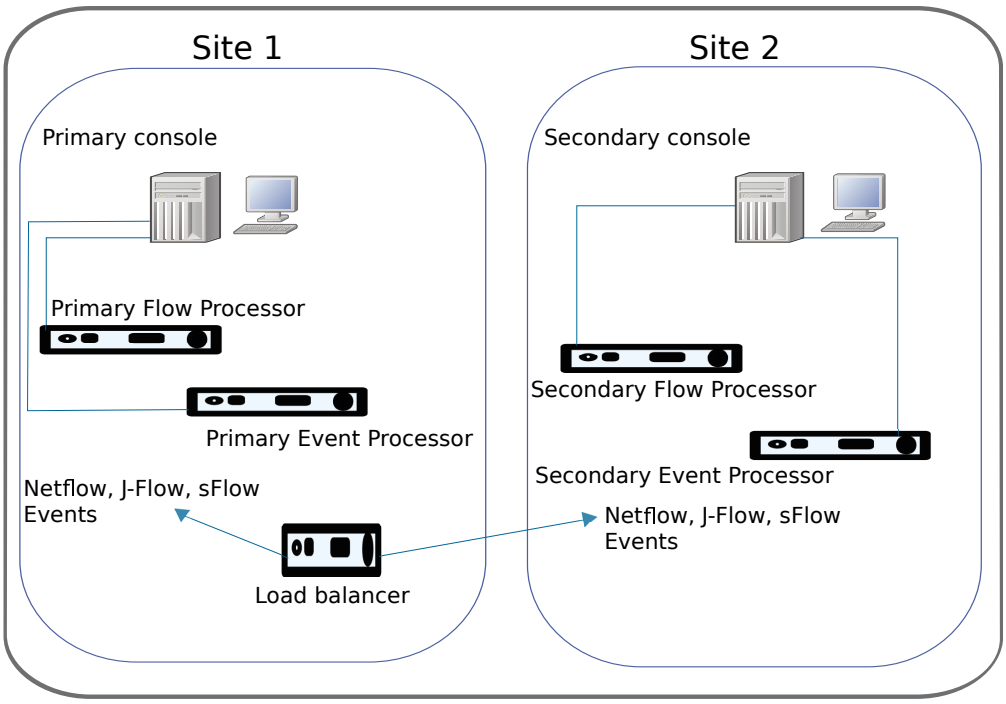

Figure 3. Sending events and flows to two sites

Configure QRadar to receive events

QRadar automatically discovers many log sources that send syslog messages in your deployment. Log sources that are automatically discovered by QRadar appear in the Log Sources window.

You configure the automatic discovery of log sources for each Event Collector by using the **Autodetection Enabled** setting in the Event Collector configuration. If you want to keep the log source event IDs synchronized with the primary Event Collector, you disable the **Autodetection** setting. In this situation, use the content management tool to synchronize the log source configuration or restore a configuration backup to the site.

For more information about auto discovered log sources and configurations specific to your device or appliance, see the *IBM Security QRadar DSM Configuration Guide* and the *IBM Security QRadar Log Sources Configuration Guide*.

Configure QRadar to receive flows

To enable data redundancy for flows, you need to send NetFlow, J-Flow, and sFlow to both sites for QFlow collection.

You can collect flows from a SPAN or tap and then send packets to your backup location, or you mirror the SPAN or tap in the backup location by using external technologies. A load balancer splits flows such as NetFlow, J-Flow, and sFlow but it can't split QFlow.

For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.

Use the Content Management Tool (CMT)

If you want to ensure that the primary QRadar Console from site 1 and the secondary QRadar Console from site 2 have identical configurations, use the content management tool to update site 2 with the configurations from site 1.

For more information about using the content management tool, see the *IBM Security QRadar SIEM Administration Guide*.

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.

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

Privacy policy considerations

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Printed in USA