IBM QRadar Security Intelligence
Version 7.2.6

Offboard Storage Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 31.

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This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.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

This guide provides information about how to move the `/store` or `/store/ariel` file systems to an external storage device for IBM® Security QRadar® products.

Intended audience

System administrators responsible for configuring offboard storage devices must have administrative access to QRadar systems and to network devices and firewalls. The system administrator must know the corporate network 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?uid=swg21616144).

Statement of good security practices

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

Please Note:

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

Chapter 1. Offboard storage overview

To increase the amount of storage space on your appliance, you can move a portion your data to an offboard storage device. You can move your `/store`, `/store/ariel`, or `/store/backup` file systems.

Multiple methods are available for adding external storage, including iSCSI, Fiber Channel, and NFS (Network File System). You must use iSCSI or Fiber Channel to store data that is accessible and searchable in the UI, such as the `/store/ariel` directory.

Important: NFS can be used only for daily backup data, such as the `/store/backup/` directory.

You can use offboard storage solutions on any managed host or console, including on high-availability (HA) systems. When you use iSCSI or Fibre Channel with HA, the external storage device is mounted by the active HA node, ensuring data consistency for an HA failure. When you use external storage with HA, you must configure these devices on the primary HA host, and on the secondary HA host.

Before you implement an offboard storage solution, consider your local storage options, existing hardware infrastructure, and your data retention and fault tolerance requirements.

Local storage

Data that is stored locally on a QRadar appliance can be accessed with lower latency than external storage and supports up to 40 TB of data. When possible, use local storage and Data Node appliances as an alternative to an external storage device.

Multiple appliances

Use multiple appliances if larger storage capacity is required for your QRadar deployment.

When multiple appliances are not feasible, or an existing deployment can increase capacity by using available external storage, then external storage might be appropriate for your deployment.

Hardware and infrastructure

Your existing infrastructure and experience with storage area networks are important factors in deciding whether to use an offboard storage solution.

Certain offboard devices require less configuration and might be able to use existing network infrastructures. For example, iSCSI uses existing Ethernet networking, while Fibre Channel uses more specialized hardware.

Data retention and fault tolerance

Your QRadar data retention policy is important in considering an offboard storage solution. If your data retention settings exceed the capacity of existing storage or

your are planning to expand the retention of existing deployed appliances, you might require an offboard storage solution.

An offboard storage solution can be used to improve your fault tolerance and disaster recovery capabilities.

File system options for offboard storage

Use an offboard storage solution to move the /store file system or specific subdirectories, such as the /store/ariel directory.

You can move the /store file system when you want to increase the fault tolerance levels in your IBM Security QRadar deployment. Each option impacts QRadar performance.

Moving the /store file system to an external device can provide an alternative to implementing a high-availability system.

The /store/ariel directory is most common file system that is moved to an offboard storage solution.. By moving the /store/ariel file system, you can move collected log and network activity data to external storage. The local disk remains used for the PostgreSQL database and temporary search results.

Administrators can move the following types of QRadar data to offboard storage devices:

- PostgreSQL metadata and configuration information
- Log activity, payloads (raw data), normalized data, and indexes
- Network activity, payloads, normalized data, and indexes
- Time series graphs (global views and aggregates)

Performance impact of offboard storage solutions

Moving the /store file system to an external device might affect QRadar performance.

After migration, all data I/O to the /store file system is no longer done on the local disk. Before you move your QRadar data to an external storage device you must consider the following information:

- Maintain your log and network activity searches on your local disk by mounting the /store/transient file system to the unused /store file partition.
- Searches that are marked as saved are also in the /store/transient directory. If you experience a local disk failure, these searches are not saved.

Storage expansion

By creating multiple volumes and mounting /store/ariel/events and /store/ariel/flows, you can expand your storage capabilities past the 16 TB file system limit that is supported by QRadar.

Any subdirectory in the /store file system can be used as a mount point for your external storage device.

If you want to move dedicated event or flow data, you might configure more specific mount points. For example, you can configure /store/ariel/events/

records and /store/ariel/events/payloads as mount points. Specific mount points can provide up to 32 TB of storage for the **Log Activity** or **Network Activity** data.

External storage options

You can use iSCSI, Fibre Channel, or NFS to provide an offboard storage solution.

Onboard disks provide a faster solution than offboard storage devices. Local disk storage on appliances supports IBM Security QRadar read speeds of 200 - 400 MBps and write speeds of almost 200 Mbps. When multiple appliances are deployed, performance and capacity scale at the same rate.

Fibre Channel
Fibre Channel provides the fastest offboard performance by using storage area network (SAN) speeds of 200 MBps to 3200 MBps, depending on your network configuration.

Fibre Channel performance might be impacted by factors within the SAN implementation, such as the following factors:

- Disk or spindle counts per volume
- Number of concurrent sessions.
- Cache capacity in the SAN controllers.

iSCSI iSCSI uses a dedicated storage channel over standard Ethernet infrastructure, rather than a dedicated SAN network. For this reason, iSCSI can be the easiest to implement, most cost effective, and most readily available.

If you implement an iSCSI solution, then network capacity is shared between external storage access and management interface I/O. In this situation, you can configure a secondary network interface on a separate storage network.

Using a dedicated interface, you are limited to 1 Gbps and might experience only 200 MBps to 400 MBps. Your iSCSI storage device might provide only 25 MBps to 50 MBps I/O performance.

NFS A Network File System (NFS) solution must not be used to store active QRadar data. You can move the /store/backup file system to an external NFS.

If the /store file system is mounted to an NFS solution, PostgreSQL data can be corrupted. If the /store/ariel file system is mounted to NFS, QRadar experiences performance issues.

Use NFS for tasks during off-peak times, tasks that involve batch file writes, and tasks that involve a limited volume of file I/O. For example, use NFS for daily configuration and data backups.

NFS storage operates over existing management Ethernet networks and is limited to performance levels of 20 MBps to 50 MBps. The NFS protocol might affect performance for file access, locking, and network permissions. Remediate the performance impact by using a dedicated network interface.

If NFS is used only for backups, the same NFS share can be used for each host. The backup files contain the system host name, which enables the identification of each backup file. If you are storing a long period of data on your NFS shares, consider a separate share or export for each appliance in your deployment.

External storage limitations

Multiple systems cannot access the same block device in an IBM Security QRadar deployment.

If you configure iSCSI in an HA environment, do not mount the iSCSI or Fibre Channel volumes on the secondary host while the primary host is accessing the volumes.

An external storage device must able to provide consistent read and write capacity of 100 MBps to 200 MBps. When consistent read and write capacity is not available, the following issues might occur:

- Data write performance is impacted.
- Search performance is impacted.

If performance continues to degrade, then the processing pipeline can become blocked and QRadar might display warning messages and drop events and flows.

Offboard storage in HA environments

If you choose to move the `/store` file system in a high-availability (HA) environment, the `/store` file system is not replicated by using Disk Replication Block Device.

If you move the `/store/ariel` file system to an offboard storage device and maintain the `/store` file system on local disk, the `/store` file system is synchronized with the secondary HA host. By default, when your environment is configured for HA, Disk Replication Block Device is enabled.

Chapter 2. iSCSI external storage device

Administrators can configure an iSCSI storage device in a standard or high-availability (HA) IBM Security QRadar deployment.

When you configure an iSCSI external storage device, you must migrate the QRadar data that is maintained on your `/store` or `/store/ariel` file system and then mount the `/store` or `/store/ariel` file system to a partition on the iSCSI device volume.

Depending on your device configuration, you might be required to create a partition on the volume of your Fibre Channel disk.

If you configure iSCSI in an HA deployment and your primary HA host fails, your iSCSI device can be used to maintain data consistency with your secondary HA host.

iSCSI configuration options in an HA environment

iSCSI configurations are different for a primary HA host and secondary HA host. To configure iSCSI you must ensure that the primary HA host and secondary HA host are not connected in an HA cluster.

In HA environments, review the `/var/log/messages` file for errors in your iSCSI storage configuration.

Ensure that you use a different **`initiatorname`** on the primary HA host and secondary HA host. Your iSCSI device must be configured to enable each **`initiatorname`** to access the same volume on the iSCSI device.

You configure the **`initiatorname`** in the `/etc/iscsi/initiatorname.iscsi` file and is used by QRadar to identify the volume on the iSCSI device where the `/store` or `/store/ariel` file system is mounted.

Related tasks:

"Configuring iSCSI in an HA deployment" on page 11
To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

Secondary network interfaces

You can configure a secondary network interface with a private IP address to connect to an iSCSI storage area network (SAN).

You use secondary network interface to improve performance. If you configure a secondary network interface, you require address information from your SAN network manager. For more information about configuring a network interface, see your *Administration Guide*.

HA systems in iSCSI deployments

For dedicated access to the iSCSI storage network, use the following order to set up high availability (HA), iSCSI, and a network interface:

1. Configure the primary and secondary appliances.
2. Set up external iSCSI storage on both hosts
3. Configure HA on the primary and secondary hosts.

The HA process for IBM Security QRadar controls the all network interfaces. When an HA appliance is in active mode, the HA process enables the interfaces. When HA is in standby mode, the HA process disables the interfaces. If the dedicated network interface for storage is disabled and the HA system goes into failover, the standby host tries to go into active mode. If the HA system is in standby mode, you cannot access the iSCSI storage system. Access issues are caused during the transition of the HA node from standby to active. The HA process brings the secondary interface online, but when the iSCSI system is mounted, the networking is not available and the failover process fails. The standby HA host cannot change to active mode.

To resolve the issue, you must remove control of the iSCSI network interface from the HA system to ensure that network interface is always active. Remove any dependencies that the network interface has on the status of the HA node. The HA primary and secondary hosts must have unique IP addresses on these secondary network interfaces.

Related tasks:

"Configuring control of secondary interfaces in HA deployments" on page 13
If you use iSCSI and a dedicated network interface in a high-availability (HA) deployment, you must ensure that the secondary interface is not managed by the HA process. Configure the management of the secondary interface to ensure that in the event of a failover to the secondary HA host, the interface always remains active.

iSCSI configuration in standard QRadar deployments

Use QRadar Console to configure iSCSI in a standard deployment.

Administrators must perform the following tasks in sequence:

1. Configure iSCSI volumes
2. Migrate the file system to an iSCSI storage solution.
   - Move the /store/ariel file system to an iSCSI storage solution.
   - Move the /store file system to an iSCSI storage solution.
   - Mount the iSCSI volume automatically
3. Verify iSCSI connections.

Configuring the iSCSI volumes

You can configure iSCSI for a stand-alone QRadar Console or a QRadar Console that is the primary high-availability (HA) host in an HA deployment.

About this task

Optionally, you can create a partition on the volume of the external iSCSI storage device.

IBM Security QRadar V7.2.1 and later uses the XFS file system. You can create the partition on your iSCSI device with either an ext4 or XFS file system.

Disk partitions are created by using GUID Partition Table (GPT). You can use a new device partition as the mount point for the file system, such as `/store` or `/store/ariel` that you migrate.

Important: If you created an iSCSI or Fibre Channel device partition on your external device and QRadar data is stored, then you cannot create a partition or reformat the partition on the volume.

Procedure

1. Using SSH, log in to the QRadar Console as the root user.
2. Edit the `/etc/iscsi/initiatorname.iscsi` file to include the iSCSI qualified name for your host.

   `InitiatorName=`*`iqn.yyyy-mm`*`.{reversed domain name}:`*`hostname`*

   Example: `InitiatorName=iqn.2014-11.com.qradar:pl13`
3. Open a session to the iSCSI server by typing the following command: `service iscsi restart`.
4. To detect volumes on the iSCSI server, type the following command:

   `iscsiadm -m discovery --type sendtargets --`*`portal IP address`*`:[`*`port`*`]`

   The *IP address* option is the IP address of the iSCSI server. The *port* is optional. Record the initiator name.
5. To log in to the ISCSI server, type the following command:

   `iscsiadm -m node --targetname <`*`Initiator name from step 4`*`> --portal <`*`IP address`*`:[`*`port`*`]> --login`
6. To find the iSCSI device volume name, type the following command:

   `dmesg | grep "Attached SCSI disk"`
7. Optional: To create a partition, use the GNU parted command:

   `parted /dev/`*`volume`*
8. Configure the partition label to use GPT by typing the following command:

   `mklabel gpt`
9. If the following message is displayed, type `Yes`.

   ```
   Warning: The existing disk label on /dev/volume will be
   destroyed and all data on this disk will be lost. Do you want to
   continue?
   ```
10. Create a partition on the iSCSI disk volume.
    a. To create the partition, type the following command:

       `mkpart primary 0% 100%`
    b. Set the default units to TB by typing the following command:

       `unit TB`
    c. Verify that the partition is created by typing the following command:

       `print`
    d. Exit from GNU parted by typing the following command:

       `quit`
    e. Update the kernel with the new partition data by typing the following command:

       `partprobe /dev/`*`volume`*

You might be prompted to restart the appliance.

f. To verify that the partition is created, type the following command:

```
cat /proc/partitions
```

11. Reformat the partition and make a file system.
    - To create an XFS file system, type the following command: `mkfs.xfs -f /dev/partition`
    - For an ext4 files system, type the following command: `mkfs.ext4 /dev/partition`

What to do next

See "Moving the /store/ariel file system to an iSCSI storage solution" or "Moving the /store file system to an iSCSI storage solution" on page 9.

Related tasks:

"Troubleshooting iSCSI issues" on page 14
To prevent iSCSI disk and communication issues, you must connect QRadar, the iSCSI server, and your network switches to a uninterruptible power supply (UPS). Power failure in a network switch might result in your iSCSI volume reporting disk errors or remaining in a read-only state.

Moving the /store/ariel file system to an iSCSI storage solution

You can migrate the IBM Security QRadar data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to an iSCSI device partition.

Before you begin

Configure iSCSI volumes.

Procedure

1. Stop the hostcontext service by typing the following command:

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

2. Move the existing mount point by typing the following commands:

```
cd /store
mv ariel ariel_old
```

3. Verify the Universally Unique Identifier (UUID) of the iSCSI device partition by typing the following command:

```
blkid /dev/partition
```

4. Add the mount point for the `/store/ariel` file system by adding the following text to the `/etc/fstab` file:
    - If the file system is ext4, add the following text

```
UUID=uuid /store/ariel ext4 noatime,noauto,nobarrier 0 0
```

    - If the file system is XFS, copy the following text into a text editor, remove the line break, and paste as a single line:

```
UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,
noauto,nobarrier 0 0
```

5. Create the ariel directory for the mount point by typing the following command:

```
mkdir ariel
```

6. Mount /store/ariel to the iSCSI device partition by typing the following command:

   ```
   mount /store/ariel
   ```

7. Verify that /store/ariel is correctly mounted by typing the following command:

   ```
   df -h
   ```

8. Move the data from the local disk to the iSCSI storage device by typing the following command:

   ```
   mv /store/ariel_old/* /store/ariel
   ```

9. Remove the /store/ariel_old directory by typing the following command:

   ```
   rmdir /store/ariel_old
   ```

10. Start the hostcontext service by typing the following command:

    ```
    service crond start
    service systemStabMon start
    service hostservices start
    service tomcat start
    service hostcontext start
    ```

What to do next

See "Mounting the iSCSI volume automatically" on page 11.

Related tasks:

"Moving the /store file system to an iSCSI storage solution"
You can migrate the IBM Security QRadar data that is maintained in the /store file system and mount the /store file system to an iSCSI device partition.

Moving the /store file system to an iSCSI storage solution

You can migrate the IBM Security QRadar data that is maintained in the /store file system and mount the /store file system to an iSCSI device partition.

Migrating the /store files system to your offboard storage device can take an extended period of time.

Before you begin

Configure iSCSI volumes..

Procedure

1. Stop the hostcontext service by typing the following command:

   ```
   service hostcontext stop
   service tomcat stop
   service hostservices stop
   service systemStabMon stop
   service crond stop
   ```

2. Unmount the file systems by typing the following commands:

   ```
   umount /store/tmp
   umount /store/transient
   umount /store
   ```

3. Create the /store_old directory by typing the following command:

   ```
   mkdir /store_old
   ```

4. Derive the iSCSI device partition universal unique identifier (UUID) by typing the following command:

```
blkid /dev/partition
```

5. Edit the /etc/fstab file to update the existing /store file system mount point to /store_old.
6. Add a new mount point for the /store file system by adding the following text to the /etc/fstab file:
   - If the file system is ext4, add the following text:

     ```
     UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
     ```
   - If the file system is XFS, add the following text:

     ```
     UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
     ```

   a. Modify the /store/tmp mount line to use the following file system options:

      ```
      noatime,noauto,nobarrier 0 0
      ```

   b. If /store/transient is listed in the fstab file, then type the following file system options:

      ```
      xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
      ```

   c. Save and close the file.
7. Mount the /store file system to the iSCSI device partition by typing the following command:

   ```
   mount /store
   ```
8. Mount the /store_old file system to the local disk by typing the following command:

   ```
   mount /store_old
   ```
9. Move the data from the local disk to the iSCSI storage device by typing the following command:

   ```
   mv -f /store_old/* /store
   ```
10. Re-mount the file systems by typing the following commands:

    ```
    mount /store/tmp
    mount /store/transient
    ```
11. Unmount /store_old by typing the following command:

    ```
    umount /store_old
    ```
12. Remove the /store_old directory from the /etc/fstab file by typing the following command:

    ```
    rmdir /store_old
    ```
13. Start the hostcontext service by typing the following command:

    ```
    service crond start
    service systemStabMon start
    service hostservices start
    service tomcat start
    service hostcontext start
    ```

What to do next

See "Mounting the iSCSI volume automatically" on page 11.

Related tasks:

"Moving the /store/ariel file system to an iSCSI storage solution" on page 8
You can migrate the IBM Security QRadar data that is maintained in the /store/ariel file system and mount the /store/ariel file system to an iSCSI device partition.

Mounting the iSCSI volume automatically

You must configure IBM Security QRadar to automatically mount the iSCSI volume.

Before you begin

Ensure that you moved the `/store/ariel` and `/store` file systems to an iSCSI storage solution.

Procedure

1. Add the iSCSI script to the startup information by typing the following commands:

   ```
   chkconfig --add iscsi
   chkconfig --level 345 iscsi on
   ```

2. Create a symbolic link to the script that mounts the iSCSI storage solution by typing the following command:

   ```
   ln -s /opt/qradar/init/iscsi-mount /etc/init.d
   ```

3. Add the mount script to the startup information by typing the following commands:

   ```
   chkconfig --add iscsi-mount
   chkconfig --level 345 iscsi-mount on
   ```

4. Verify that the iSCSI device is correctly mounted by restarting your system.
   a. Restart the system by typing the following command: `reboot`
   b. Ensure that the iSCSI mount point is retained by typing the following command: `df -h`

What to do next

If you are configuring a high-availability (HA) environment, you must set up your secondary HA host by using the same iSCSI connections that you used for your primary HA host. For more information, see "Configuring iSCSI in an HA deployment."

Related tasks:

"Configuring iSCSI in an HA deployment"
To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

Configuring iSCSI in an HA deployment

To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

Procedure

1. Using SSH, log in to the secondary HA host as the root user.
2. To configure your HA secondary host to identify the iSCSI device volume, add the iSCSI qualified name for your host to the `/etc/iscsi/initiatorname.iscsi` file.

   `Initiatorname=iqn.`*`yyyy-mm`*`.{reversed domain name}:`*`hostname`*

   Example: `InitiatorName=iqn.2008-11.com.qradar:pl13`

3. Restart the iSCSI service to open a session to the server by typing the following command:

   ```
   service iscsi restart
   ```

4. To detect the volume on the iSCSI server, type the following command:

   ```
   iscsiadm -m discovery --type sendtargets --portal IP address:[port]
   ```

   Note: The *port* is optional.

5. Verify the login to your iSCSI server by typing the following command:

   ```
   iscsiadm -m node -l
   ```

6. To find the iSCSI device volume name, type the following command:

   ```
   dmesg | grep "Attached SCSI disk"
   ```

7. Optional: To create a partition, use the GNU parted command:

   ```
   parted /dev/volume
   ```

8. Configure the mount point for the secondary HA host.
   a. To unmount the file systems, type the following commands:

      ```
      umount /store/tmp
      umount /store/transient
      umount /store
      ```

   b. Identify the UUID of the iSCSI device partition by typing the following command:

      ```
      blkid /dev/partition
      ```

   c. If you are moving the /store file system, edit the file settings in the /etc/fstab file to be the same as the mount points that are listed in the /etc/fstab file on the HA primary host:
      - /store
      - /store/temp
      - /store/transient

   d. If you are moving the /store/ariel file system, edit the settings in the /etc/fstab file to be the same as the mount point that is listed in the /etc/fstab file on the HA primary host for /store/ariel.

9. Configure the secondary HA host to automatically mount the iSCSI volume.
   a. Add the iSCSI script to the startup information by typing the following commands:

      ```
      chkconfig --add iscsi
      chkconfig --level 345 iscsi on
      ```

   b. Create a symbolic link to the mount script by typing the following command:

      ```
      ln -s /opt/qradar/init/iscsi-mount /etc/init.d
      ```

   c. Add the mount script to the startup information by typing the following commands:

      ```
      chkconfig --add iscsi-mount
      chkconfig --level 345 iscsi-mount on
      ```

What to do next

See "Verifying iSCSI connections" on page 14.

Related concepts:

"iSCSI configuration options in an HA environment" on page 5
iSCSI configurations are different for a primary HA host and secondary HA host. To configure iSCSI you must ensure that the primary HA host and secondary HA

host are not connected in an HA cluster.

Configuring control of secondary interfaces in HA deployments

If you use iSCSI and a dedicated network interface in a high-availability (HA) deployment, you must ensure that the secondary interface is not managed by the HA process. Configure the management of the secondary interface to ensure that in the event of a failover to the secondary HA host, the interface always remains active.

Before you begin

Ensure that the following conditions are met:

- Separate IP addresses for the dedicated iSCSI network interface on each of the HA servers

  Separate IP addresses prevent IP address conflicts when the network interfaces are active on both HA hosts at the same time. The iSCSI software and drivers can access the external storage at startup and during the HA failover. Also, the external volume can be successfully mounted when the HA node switches from standby to active.
- The primary and secondary appliances are configured.

  For more information, see the *IBM Security QRadar High Availability Guide*
- iSCSI storage is configured.

Procedure

1. On the primary host, use SSH to log in to the QRadar Console as the root user.
2. Disable the QRadar HA service control of network interface.
   a. Go to the `/opt/qradar/ha/interfaces/` directory

      The directory contains a list of files that are named `ifcfg-ethN`. One file exists for each interface that is controlled by QRadar HA processes.
   b. Delete the file that is used to access your ISCSI storage network.

      Deleting the file removes control of the interface from the HA processes.
3. Re-enable operating system-level control of the network interfaces.
   a. Go to the `/etc/sysconfig/network-scripts/ifcfg-ethN` directory.
   b. Open the `ifcfg-ethN` file for the interface that connects to your ISCSI network.
   c. To ensure that the network interface is always active, change the value for the `ONBOOT` parameter to `ONBOOT=yes`.
4. To restart the iSCSI services, type the following command:

   ```
   /etc/init.d/iscsid restart
   ```
5. Repeat these steps for the HA secondary appliance.
6. Optional: To test access to your ISCSI storage from your secondary appliance, use the ping command:

   ```
   ping iscsi_server_ip_address
   ```

Related concepts:

"Secondary network interfaces" on page 5
You can configure a secondary network interface with a private IP address to connect to an iSCSI storage area network (SAN).

Verifying iSCSI connections

Verify that the connections between a primary HA host or secondary HA host and an iSCSI device are operational

Procedure

1. Using SSH, log in to the primary or secondary HA host as the root user.
2. To test the connection to your iSCSI storage device, type the following command:

   `ping iSCSI_Storage_IP_Address`
3. Verify the iSCSI service is running and that the iSCSI port is available by typing the following command:

   `telnet iSCSI_Storage_IP_Address 3260`

   Note: The default pot is 3260.
4. Verify that the connection to the iSCSI device is operational by typing the following command:

   `iscsiadm -m node`

   To verify that the iSCSI device is correctly configured, you must ensure that the output that is displayed for the primary HA host matches the output that is displayed for the secondary HA host.

   If the connection to your iSCSI volume is not operational, the following message is displayed:

   `iscsiadm: No records found`
5. If the connection to your iSCSI volume is not operational, then review the following troubleshooting options:
   - Verify that the external iSCSI storage device is operational.
   - Access and review the /var/log/messages file for specific errors with your iSCSI storage configuration.
   - Ensure that the iSCSI **initiatornames** values are correctly configured by using the `/etc/iscsi/inititatornames.iscsi` file.
   - If you cannot locate errors in the error log, and your iSCSI connections remain disabled, then contact your Network Administrator to confirm that your iSCSI server is functional or to identify network configuration changes.
   - If your network configuration has changed, you must reconfigure your iSCSI connections.

What to do next

Establish an HA cluster. You must connect your primary HA host with your secondary HA host by using the QRadar user interface. For more information about creating an HA cluster, see the *IBM Security QRadar High Availability Guide*.

Troubleshooting iSCSI issues

To prevent iSCSI disk and communication issues, you must connect QRadar, the iSCSI server, and your network switches to a uninterruptible power supply (UPS). Power failure in a network switch might result in your iSCSI volume reporting disk errors or remaining in a read-only state.

.

About this task

In a high-availability (HA) environment, if your primary host fails, you must restore your iSCSI configuration to the primary host. In this situation, the `/store` or `/store/ariel` data is already migrated to the iSCSI shared external storage device. Therefore, to restore the primary host iSCSI configuration, ensure that you configure a secondary HA host. For more information see, "Configuring iSCSI in an HA deployment" on page 11

Procedure

1. Determine whether there is a disk error.
   a. Using SSH, log in to QRadar Console as the root user.
   b. Create an empty file named `filename.txt` on your iSCSI volume by typing one of the following command:
      - `touch /store/ariel/filename.txt`
      - `touch /store/filename.txt`

   If your iSCSI volume is mounted correctly and you have write permissions to the volume, the touch command creates an empty file named filename.txt on your iSCSI volume.

   If you see an error message, unmount and remount the iSCSI volume.
2. Stop the IBM Security QRadar services.
   - If you migrated the /store file system, type the following commands in the specified order:
     - `service hostcontext stop`
     - `service tomcat stop`
     - `service hostservices stop`
     - `service systemStabMon stop`
     - `service crond stop`
   - If you migrated the `/store/ariel` file system, type the following command:
     `service hostcontext stop`
3. Unmount the iSCSI volume.
   - If you migrated the `/store` file system, type the following commands:
     - `umount /store/tmp`
     - `umount /store`
   - If you migrated the `/store/ariel` file system, type the following command:
     `umount /store/ariel`
4. Mount the iSCSI volume.
   - If you migrated the `/store` file system, type the following commands:
     `mount /store`
     `mount /store/tmp`
   - If you migrated the `/store/ariel` file system, type the following command:
     `mount /store/ariel`
5. Test the mount points.
   - If you migrated the `/store` file system, type the following command:
     `touch /store/filename.txt`
   - If you migrated the `/store/ariel` file system, type the following command:
     `mount /store/ariel/filename.txt`

If you continue to receive a read-only error messages after remounting the disk, then reconfigure your iSCSI volume.

Alternatively, you can unmount the file system again and run a manual file system check with the following command: `fsck /dev/partition`.

6. Start the QRadar services.
   - If you migrated the `/store` file system, type the following commands in the specified order:
     - `service crond start`
     - `service systemStabMon start`
     - `service hostservices start`
     - `service tomcat start`
     - `service hostcontext start`
   - If you migrated the `/store/ariel` file system, type the following command: `service hostcontext start`

Related tasks:

"Configuring the iSCSI volumes" on page 6
You can configure iSCSI for a stand-alone QRadar Console or a QRadar Console that is the primary high-availability (HA) host in an HA deployment.

Chapter 3. Fibre Channel storage

You can configure Fibre Channel (FC) in a standard QRadar deployment or in a high-availability (HA) environment. You can also configure FC multipath to provide redundancy if your FC switch fails.

When you configure an FC device, you can move the IBM Security QRadar data in your `/store` or `/store/ariel` file system. Then, mount the `/store` or `/store/ariel` file system to a partition on the FC device.

Depending on your device configuration, you might be required to create a partition on the volume of your FC disk.

If you configure FC in an HA deployment and your primary HA host fails, your FC device can be used to maintain data consistency with your secondary HA host. For more information about data consistency and shared storage in an HA environment, see the *IBM Security QRadar High Availability Guide*.

Configuration overview for Fibre Channel storage

Configuring Fibre Channel (FC) is different for a primary high-availability (HA) host than the secondary HA host. To configure FC, you must ensure that the primary HA host and secondary HA host are not connected in an HA cluster.

Frequently searched data must be moved to a faster disk. For example, move recent data or data that is used for security incident investigations. However, deploying high performance offboard disk storage might be costly. Where possible, use lower performance and less expensive offboard storage for activities such as moving older data, archiving, or for reporting purposes.

If you are using FC only for archive purposes, then use the same mount point for every appliance and configure these mount points to correspond with each unique FC volume.

In deployments that use multiple appliances, ensure that each appliance is configured to use a separate FC volume. Failure to use separate volumes can result in two devices that mount the same block device, which can corrupt the block device file system.

Verifying your Emulex adapter installation

You must verify that an Emulex LPe12002 Host Bus adapter is attached and installed with the correct firmware and driver versions.

Before you begin

To use the Fibre Channel protocol, you must install an Emulex LPe12002 Host Bus adapter on your IBM Security QRadar appliance. In a high-availability (HA) deployment, you must install an Emulex LPe12002 card on the primary and secondary HA host.

The Emulex LPe Host Bus adapter must use the following driver and firmware versions:

- Driver version: 8.3.5.68.5p
- Firmware version: 1.10A5(U3D1.10A5),sli-3

Procedure

1. Using SSH, log in to your QRadar host as the root user:
2. Verify that an Emulex LPe12002 card is attached by typing the following command:

   ```
   hbacmd listhbas
   ```

   If no result is displayed, then contact your system administrator.
3. Verify that the Emulex card is using the correct firmware and driver versions by typing the following command:

   ```
   hbacmd HBAAttrib
   ```

   device id is the Port WWN that is displayed in the preceding step.

Related tasks:

"Verifying the Fibre Channel connections"
You must identify the disk volume on the external Fibre Channel device. If required, you must also create a partition on the volume.

Verifying the Fibre Channel connections

You must identify the disk volume on the external Fibre Channel device. If required, you must also create a partition on the volume.

Before you begin

Verify your Emulex adapter installation.

Procedure

1. Using SSH, log in to your QRadar Console as the root user.
2. Identify the Fibre Channel volume by typing the following command:

   ```
   ls -l /dev/disk/by-path/*-fc-*
   ```

   If multiple Fibre Channel devices are attached and you cannot identify the correct Fibre Channel volume, contact your system administrator.
3. Optional: If there is no partition on the Fibre Channel volume, then create a partition on the Fibre Channel device volume.
   a. Optional: To create a partition, use the GNU parted command:

      ```
      parted /dev/volume
      ```

   b. Configure the partition label to use GPT by typing the following command:

      ```
      mklabel gpt
      ```

   c. If the following message is displayed, type `Yes`.

      ```
      Warning: The existing disk label on /dev/volume will be
      destroyed and all data on this disk will be lost. Do you want to
      continue?
      ```

   d. To create the partition, type the following command:

      ```
      mkpart primary 0% 100%
      ```

   e. Set the default units to TB by typing the following command:

      ```
      unit TB
      ```

   f. Verify that the partition is created by typing the following command:

      ```
      print
      ```

   g. Exit from GNU parted by typing the following command:

```
quit
```

h. Update the kernel with the new partition data by typing the following command:

```
partprobe /dev/volume
```

You might be prompted to restart the appliance.

i. To verify that the partition is created, type the following command:

```
cat /proc/partitions
```

4. Reformat the partition and make a file system.
   - To create an XFS file system, type the following command: `mkfs.xfs -f /dev/partition`
   - For an ext4 files system, type the following command: `mkfs.ext4 /dev/partition`

Related tasks:

"Verifying your Emulex adapter installation" on page 17
You must verify that an Emulex LPe12002 Host Bus adapter is attached and installed with the correct firmware and driver versions.

Moving the /store file system to a Fibre Channel solution

You can move the IBM Security QRadar data that is maintained in the `/store` file system and mount the `/store` file system to a Fibre Channel (FC) device partition.

Before you begin

"Verifying the Fibre Channel connections" on page 18

Procedure

1. After the QRadar installation, connect QRadar with fibre channel and restart.
2. Stop the `hostcontext` service by typing the following command:

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

3. Unmount the file systems by typing the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

The `/store/transient` file system is mounted only when the `/store file system` is XFS.

4. Create the `/store_old` directory by typing the following command:

```
mkdir /store_old
```

5. Derive the device partition universal unique identifier (UUID) by typing the following command:

```
blkid /dev/partition
```

6. Edit the `/etc/fstab` file to update the existing `/store` file system mount point to `/store_old`.
7. Add a mount point for the `/store` file system by adding the following text to the `/etc/fstab` file:
   - If the file system is ext4, add the following text

     ```
     UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
     ```

   - If the file system is XFS, add the following text:

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

a. Modify the `/store/tmp` mount line to use the following file system options:

```
noatime,noauto,nobarrier 0 0
```

b. If `/store/transient` is listed in the `fstab` file, then type the following file system options:

```
xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

c. Save and close the file.

8. Mount the `/store` file system to the FC device partition by typing the following command:

```
mount /store
```

9. Mount the `/store_old` file system to the local disk by typing the following command:

```
mount /store_old
```

10. Copy the data to the Fibre Channel partition by typing the following command:

```
cp -af /store_old/* /store
```

11. Mount the file systems by typing the following commands:

```
mount /store/tmp
mount /store/transient
```

The `/store/transient` file system is mounted only when the`/store` file system is XFS.

12. Unmount `/store_old` by typing the following command:

```
umount /store_old
```

13. Remove the `/store_old` directory from the `/etc/fstab` file.
14. Start the `hostcontext` service by typing the following command:

```
service crond start
service systemStabMon start
service hostservices start
service tomcat start
service hostcontext start
```

What to do next

See "Verifying the Fibre Channel mount point" on page 22.

Related tasks:

"Moving the /store/ariel file system to a Fibre Channel solution"
You can move the IBM Security QRadar data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to a Fibre Channel (FC) device partition.

Moving the /store/ariel file system to a Fibre Channel solution

You can move the IBM Security QRadar data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to a Fibre Channel (FC) device partition.

Before you begin

See "Verifying the Fibre Channel connections" on page 18.

Procedure

1. After the QRadar installation, connect QRadar with fibre channel and restart.
2. Stop the QRadar services by typing the following commands:

   ```
   service systemStabMon stop
   service hostcontext stop
   service tomcat stop
   service hostservices stop
   service crond stop
   ```

3. Create a temporary directory by typing the following command:

   ```
   mkdir /tmp/fcdata
   ```

4. Mount the Fibre Channel storage partition to the temporary directory by typing the following command:

   ```
   mount /dev/<partition> /tmp/fcdata
   ```

   Where <*partition*> is the name of the device partition. For example: `sdb1`.
5. Copy the data to the Fibre Channel device by typing the following command:

   ```
   cp -af /store/ariel/* /tmp/fcdata
   ```

6. Unmount the Fibre Channel partition by typing the following command:

   ```
   umount /tmp/fcdata
   ```

7. Verify the Universally Unique Identifier (UUID) of the iSCSI device partition by typing the following command:

   ```
   blkid /dev/<partition>
   ```

   Where <*partition*> is the name of the device partition. For example: `sdb1`.
8. Edit the `fstab` file by typing the following command: `vi /etc/fstab`
9. Add the mount point for the `/store/ariel` file system by adding the following text to the `/etc/fstab` file.

   If the file system is ext4:

   ```
   UUID=uuid /store/ariel ext4 defaults,noatime,nobarrier 1 2
   ```

   If the file system is XFS:

   ```
   UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,nobarrier 0
       0
   ```

   Where *uuid* is the UUID of the fibre channel device partition.
10. Save and close the file.
11. Mount the `/store/ariel` file system to the FC device partition by typing the following command:

    ```
    mount /store/ariel
    ```

12. Start the QRadar services by typing the following commands:

    ```
    service crond start
    service hostservices start
    service tomcat start
    service hostcontext start
    service systemStabMon start
    ```

What to do next

"Verifying the Fibre Channel mount point" on page 22.

Related tasks:

"Moving the /store file system to a Fibre Channel solution" on page 19
You can move the IBM Security QRadar data that is maintained in the `/store` file system and mount the `/store` file system to a Fibre Channel (FC) device partition.

Verifying the Fibre Channel mount point

On the primary host, verify that the file system that you moved is correctly mounted to Fibre Channel device partition.

About this task

Procedure

1. Type the following command:
   ```
   df -h
   ```
2. Verify that the `/store` or `/store/ariel` file system is correctly mounted to the Fibre Channel device partition.

Configuring Fibre Channel in a standard QRadar deployment

In IBM Security QRadar, you can implement multipath Fibre Channel. If you experience a storage area network or SAN switch issue, multipath provides extra redundancy to prevent disruption to flow and event data.

Before you begin

Ensure that you completed the following tasks:

- Verify your Emulex adapter installation.
- Verify the Fibre Channel connections.

Procedure

1. On your QRadar Console appliance, attach both Fibre Channel cables to the Emulex LPe12002 Host Bus adapter.
2. Using SSH, log in to your QRadar Console as the root user:
3. Identify a storage area network (SAN) partition by typing the following command:
   ```
   blkid -o list
   ```
4. Format the partition.
   - If your file system is ext4, then type the command: `mkfs.ext4 -L multiPath /dev/`*`partition`*
   - If your file system is XFS, then type the command: `mkfs.xfs -L multiPath /dev/`*`partition`*
5. Stop the QRadar services by typing the following commands in the order specified:
   ```
   service systemStabMon stop
   service hostcontext stop
   service tomcat stop
   service imq stop
   service postgresql stop
   service hostservices stop
   ```
6. Unmount the file systems by typing the following commands:
   ```
   umount /store/tmp
   umount /store/transient
   umount /store
   ```
7. Create a `/store_old` directory by typing the following command:
   ```
   mkdir /store_old
   ```
8. Determine the Universally Unique Identifier (UUID) of the device partition by typing the following command:

```
blkid /dev/partition
```

9. Edit the /etc/fstab file.
   a. Replace the existing /store file system entry to /store_old system.
   b. If your file system is ext4, add the following text:
      ```
      UUID=uuid /store ext4 defaults,noatime,nobarrier 1 2
      ```
   c. If your file system is XFS, add the following text:
      ```
      UUID=uuid /store xfs defaults,noatime,nobarrier 1 2
      ```
10. Mount the file systems and copy the data to your device by typing the following commands:
    ```
    mount /store
    mount /store_old
    cp -af /store_old/* /store
    mount /store/tmp
    umount /store_old
    ```
11. Start QRadar services by typing the following commands in the order specified:
    ```
    service hostservices restart
    service postgresql restart
    service imq restart
    service tomcat restart
    service hostcontext restart
    service systemStabMon restart
    ```
12. Enable Fibre Channel multipath by typing the following command:
    ```
    mpathconf --enable
    ```
13. Start the multipath daemon by typing the following command:
    ```
    service multipathd start
    ```
14. Restart the system by typing the following command:
    ```
    reboot
    ```

Configuring Fibre Channel in an HA deployment

To use Fibre Channel storage, or multipath, in a high-availability (HA) environment, administrators must configure the primary HA host and the secondary HA host to use the same storage partition.

About this task

Important: You must configure multipath on both the primary and secondary HA hosts before you initiate HA syncing.

Procedure

1. Verify that the correct Fibre Channel hardware is installed on your secondary HA. For more information, see “Verifying your Emulex adapter installation” on page 17
2. Configure Fibre Channel on your primary HA host. For more information, “Configuring Fibre Channel in a standard QRadar deployment” on page 22
3. Verify the HA Fibre Channel connections. For more information, see “Verifying the Fibre Channel connections” on page 18
4. Configure the file system mount point for the secondary HA host.
5. Enable Fibre Channel multipath service if the fibre channel is configured with multipath. For more information, see “Configuring Fibre Channel in a standard QRadar deployment” on page 22.

Important: Before you add HA to a Fiber Channel configuration, confirm that `/store/backup/` is local. Create links to `/store/backup` only after adding HA.

Configuring the mount point for the secondary HA host

You must configure the mount point on the secondary high-availability (HA) host for the file system that is moved to a Fibre Channel storage device.

Procedure

1. Using SSH, log in to the secondary HA host as the root user.
2. Derive the UUID by typing the following command:

   `blkid /dev/`*`partition`*
3. Update the kernel with the Fibre Channel partition data by typing the following command: `partprobe`

   Troubleshoot: If you see a warning error message that the kernel cannot read the partition table, type the following command: `ls -l /dev/disk/by-uuid/`*`UUID`*. If no output is displayed, then restart the secondary HA host by typing `reboot`.
4. Unmount the file systems by typing the following commands:

   ```
   umount /store/tmp
   umount /store/transient
   umount /store
   ```

   The `/store/transient` file system is mounted only when the `/store` file system is XFS.
5. If you redirected the `/store` file system to an offboard device, then choose one of the following options:, edit the `/etc/fstab` file.
   - If the `/store` file system is an XFS file system, update the following lines. For each line, copy the text into a text editor, remove any line breaks, and paste as a single line.

     ```
     UUID=uuid /store xfs inode64,logbsize=256k,noatime,
     noauto,nobarrier 0 0

     UUID=uuid /store/transient xfs inode64,logbsize=256k,noatime
     ,noauto,nobarrier 0 0

     UUID=uuid /store/tmp ext4 noatime,noauto,nobarrier 0 0
     ```
   - If the `/store` file system is ext4, update the following line:

     ```
     UUID=uuid /store ext4 defaults,noatime,noauto,nobarrier 1 2
     ```
6. If you are moving the `/store/ariel` file system to an offboard device, choose one of the following options to edit the `/etc/fstab` file
   - If the `/store/ariel` file system is an XFS file system, update the following lines. For each line, copy the text into a text editor, remove any line breaks, and paste as a single line.

     ```
     UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,
     noauto,nobarrier 0 0

     UUID=uuid /store/transient xfs inode64,logbsize=256k,noatime
     ,noauto,nobarrier 0 0
     ```
   - If the `/store/ariel` file system is ext4, update the following line:

     ```
     UUID=uuid /store/ariel ext4 defaults,noatime,noauto,nobarrier 1 2
     ```

What to do next

Create an HA cluster. For more information, see *IBM Security QRadar High Availability Guide*.

Chapter 4. NFS offboard storage device

You can back up the IBM Security QRadar data to an external Network File System (NFS).

You cannot use NFS for storing active data, which includes the PostgreSQL and ariel databases. If you do use NFS, it might cause database corruption or performance issues.

Depending on your high-availability (HA) deployment, you might be required to change the location of your QRadar backup files and configure your NFS share with this new location.

You can move backup files to NFS from a stand-alone QRadar Console, configure a new HA deployment, and move backup files to NFS or move backup files from an existing QRadar HA deployment.

Moving backups to an NFS

You can configure Network File System (NFS) for a stand-alone QRadar Console, new QRadar HA deployments, or existing QRadar HA deployments.

About this task

You must enable the connections to your NFS server for any of the following situations:

- You migrate the `/store/backup` file system to NFS from a stand-alone QRadar Console
- You have new and existing HA deployments

You must configure your NFS mounts for any of the following situations:

- If you are migrating the `/store/backup` file system to NFS from a stand-alone QRadar Console.
- If you are configuring an HA deployment for the first time, then you must configure an NFS mount point for the `/store/backup` file system on your primary and secondary HA hosts.

To use NFS storage in an HA environment, you must configure the primary HA host and the secondary HA host with the same NFS configurations.

Procedure

1. Using SSH, log in to QRadar as the root user.
2. Add your NFS server to the `/etc/hosts` file:
   IP address hostname
3. Add the following line to the `/opt/qradar/conf/iptables.pre` file:
   `-A INPUT -i` *interface* `-s` *IP address* `-j ACCEPT`
   If you have a dedicated NFS network, *interface* is ETH0 or ETH1
   IP address is the IP address of your NFS server.
4. To update the firewall settings, type the following command:

```
/opt/qradar/bin/iptables_update.pl
```

5. Add NFS to be part of the startup routine by typing the following commands:

```
cd /etc/rc3.d
chkconfig --level 3 nfs on
chkconfig --level 3 nfslock on
```

6. Start NFS services by typing the following commands:

```
service nfslock start
service nfs start
```

7. Add the following line to the /etc/fstab file.

```
hostname:shared_directory/store/backup nfs
soft,intr,rw,clientaddr=IP address 0 0
```

You might need to adjust the settings for the NFS mount point to accommodate your configuration.

Example:

```
hostname:shared directory/store/backup
nfs soft,intr,rw,noac 0 0
```

8. Move your backup files from the existing directory to a temporary location by typing the following commands:

```
cd /store/
mv backup backup.local
```

9. Create a new backup directory by typing the following command:

```
mkdir /store/backup
```

10. Set the permissions for the NFS volume by typing the following command:

```
chown nobody:nobody /store/backup
```

11. Mount the NFS volume by typing the following command:

```
mount /store/backup
```

The root user must have read and write access to the mounted NFS volume because the hostcontext process runs as root user.

12. Verify that /store/backup is mounted by typing the following command:

```
df- h
```

13. Move the backup files from the temporary location to the NFS volume by typing the following command:

```
mv /store/backup.local/* /store/backupHost/inbound/
```

14. Remove the backup.local directory by typing the following commands:

```
cd /store
rm -rf backup.local
```

Configuring a new backup location

If you have an existing high-availability cluster, then you must change the IBM Security QRadar backup location on your primary HA host.

Procedure

1. Using SSH, log in to the QRadar Console as the root user:.
2. Create a file location to store your QRadar backups.

Restriction: Do not create your new backup location under the /store file system.

3. Add the following line to the /etc/fstab file.

```
hostname:shared_directory backup location nfs
soft,intr,rw,clientaddr=IP address 0 0
```

4. Mount the new backup file location to the NFS share by typing the following command:

   ```
   mount backup location
   ```

5. Copy the existing backup data to the NFS share by typing the following command:

   ```
   mv /store/backup/* backup location
   ```

6. Log in to QRadar
7. Click the **Admin** tab.
8. On the navigation menu, click **System Configuration**.
9. Click **Backup and Recovery**.
10. On the toolbar, click **Configure**.
11. In the **Backup Repository Path** field, type the location where you want to store your QRadar V7.2.2 backup files and click **Save**.
12. On the **Admin** tab menu, click **Deploy Changes**.

Configuring a mount point for a secondary HA host

On your existing secondary high-availability (HA) host, you must configure an NFS mount point for the alternative IBM Security QRadar backup file location.

Procedure

1. Using SSH, log in to the QRadar secondary HA host as the root user:
2. Create a backup file location that matches the backup file location on your primary HA host.

   For more information, see “Configuring a new backup location” on page 28.

   Restriction: Do not create your new backup location under the `/store` file system.

3. Add the following line to the `/etc/fstab` file:

   ```
   hostname:shared_directory backup location nfs
   soft,intr,rw,clientaddr=IP address 0 0
   ```

4. Mount the new QRadar backup file location by typing the following command:

   ```
   mount backup location
   ```

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.

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

Privacy policy considerations

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

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

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

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

Index

Special characters

C

D

E

F

H

I

M

N

P

S

T

Printed in USA