IBM Security QRadar
Version 7.1.0 (MR1)

# *Reconfiguring Offboard Storage During a QRadar Upgrade Technical Note*

**Note:** Before using this information and the product that it supports, read the information in Notices and Trademarks on page 15.

# CONTENTS

# 1 RECONFIGURING OFFBOARD STORAGE DURING AN UPGRADE

Connections and configurations to your offboard storage devices are not maintained when you upgrade to IBM Security QRadar SIEM 7.1.

This technical note provides information on how to reconfigure iSCSI, Fibre Channel, and NFS storage devices and complete the upgrade to QRadar SIEM 7.1.

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection. References to flows do not apply to QRadar Log Manager.

This section includes the following topics:



## Before you Begin

We recommend you review the following information before completing your upgrade to QRadar SIEM 7.1.

- During the upgrade you will be prompted to reconfigure your offboard storage devices. The message that is displayed may resemble the following:

```
The upgrade has been halted so that these mounts:  /store can
be fixed.  See/var/log/setup-7.1.0.377154/qradar_netsetup.log
for more details.

Please attach all devices and mount in accordance with product
documentation.

A copy of the pre-upgrade /etc/fstab is available for
reference: /store/tmp/710/original_fstab

Once mounts are restored, run the '/root/complete_upgrade.sh'
script to complete the upgrade.
```

Ensure you reconfigure the connections to your external storage devices before completing the upgrade. For more information about completing the upgrade, see **Completing the Upgrade to QRadar SIEM 7.1**.

- To reconfigure your iSCSI or Fibre Channel external storage device, you must modify the new /etc/fstab file. You can view a copy of the original /etc/fstab file at the following location: `/store/tmp/710/original_fstab`.
- If you migrated the /store file system to an external iSCSI or Fibre Channel device using QRadar SIEM 7.0, the QRadar SIEM 7.1 upgrade may prompt you to mount the /store_old directory. You should remove the reference to /store_old.

  To remove references to /store_old:

  - Edit the /mounts file by typing the following command:

    **`vi /tmp/restore_run_state/mounts`**

  - Remove the line `/store_old`.
  - Save and close the file.

## Reconfiguring an iSCSI Device

If you migrated the /store or /store/ariel file system to an external iSCSI device, you must reconfigure the connections to your iSCSI device during the upgrade to QRadar SIEM 7.1. After you have you reconfigured the connections you should complete the QRadar SIEM upgrade. For more information, see **Completing the Upgrade to QRadar SIEM 7.1**

**CAUTION**

*Data loss will occur if you reformat the iSCSI device partition on which the /store or /store/ariel file system was mounted before upgrading to* QRadar SIEM *7.1.*

This section includes the following topics:

- **Reconnect QRadar SIEM to the iSCSI Network**
- **Assign and configure the iSCSI volumes**
- **Reconfigure the iSCSI Device Mount Points**
- **Reconfigure QRadar SIEM to Auto-mount the iSCSI Volume**

### Reconnect QRadar SIEM to the iSCSI Network

Prepare QRadar SIEM to connect to your iSCSI network:

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

Username: **`root`**

Password:**`<password>`**

**Step 2** Configure your system to identify the iscsi device volume:

a. Open the initiatorname.iscsi file for editing by typing the following command:

```
vi /etc/iscsi/initiatorname.iscsi
```

b. Edit the file with the iSCSI qualified name for your host. Type the following:

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

For example:

```
InitiatorName=iqn.2008-11.com.q1labs:pl13
```

c. Save and close the file.

**Step 3** Open a session to the iSCSI server by typing the following command:

```
service iscsi restart
```

You are now ready to assign and configure the iSCSI volumes. See **Assign and configure the iSCSI volumes**

## Assign and configure the iSCSI volumes

To assign and configure your iSCSI volume:

**Step 1** Detect volumes on the iSCSI server by typing the following command:

```
iscsiadm -m discovery --type sendtargets --portal <IP address>:<port>
```

Where:

**<IP address>** is the IP address of the iSCSI server.

**<port>** is the port number of the iSCSI server. This is an optional parameter.

The output should resemble the following:

```
172.16.151.142:3260,1 iqn.2008-10.lab.q1labs:iscsiVol1
```

**Step 2** Verify that the login to the iSCSI server is functional by typing the following command:

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

The output should resemble the following:

```
Logging in to [iface: default, target:
iqn.2008-10.lab.q1labs:iscsiVol, portal: 172.16.151.142,3260]
Login to [iface: default, target:
iqn.2008-10.lab.q1labs:iscsiVol, portal: 172.16.151.142,3260]:
successful
```

**Step 3** Determine the iSCSI device name:

a. Clear the kernel ring buffer by typing the following command:

```
dmesg -c
```

b. Reload the iSCSI service by typing the following command:

```
service iscsi restart
```

c. Locate the device name by typing the following command:

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

The output should resemble the following:

```
sd 4:0:0:0: [sdb] Attached SCSI disk
```

Where [sdb] is the device volume.

### Reconfigure the iSCSI Device Mount Points

To configure the iSCSI device mount points:

**Step 1** Verify the Universally Unique Identifier (UUID) of the iSCSI device partition by typing the following command:

```
blkid /dev/<device name>
```

Where **<device name>** is the name of the iSCSI device volume including the partition number. For example: **sdb1**

The output should resemble the following:

```
/dev/sdb1: UUID="89ec181b-dcd1-4698-b1ae-9f1b1b044f62"
```

**Step 2** Reconfigure the /store or /store/ariel mount points using the /etc/fstab file:

**a** Open the fstab file for editing by typing the following command:

```
vi /etc/fstab
```

**b** Add the mount line for the file system that you migrated to the iSCSI device before you upgraded QRadar SIEM.

```
UUID=<uuid> <directory> <file system>
noatime,noauto,nobarrier 0 0
```

Where:

**<uuid>** is the value derived in **Step 1**.

**<directory>** is either the /store or store/ariel file system.

**<file system>** is the version you used to format the file system. For example: **ext4.**

**c** Save and close the file.

**Step 3** If you migrated the /store file system to the iSCSI device before you upgraded QRadar SIEM, go to **Step 4**.

If you migrated the /store/ariel file system to the iSCSI device before you upgraded QRadar SIEM, go to **Step 5**.

**Step 4** Mount the /store file system on the iscsi device partition:

**a** Identify the file systems that should be unmounted before you mount /store by typing the following command:

```
mount | grep ' on /store' | cut -d' ' -f3 | sort -r
```

**b** Unmount each file system in the order that they are displayed:

For example: **umount /store/tmp**.

**c** Mount the /store file system by typing the following command:

```
mount /store
```

**d** Remount, in reverse order, the file systems that were unmounted in step **b**.

**Step 5** Mount the /store/ariel file system on the iscsi device partition:

**a** Identify the file systems that should be unmounted before you mount /store/ariel by typing the following command:

```
mount | grep ' on /store/ariel' | cut -d' ' -f3 | sort -r
```

**b** Unmount each file system in the order that they are displayed.

**c** Mount the /store/ariel file system by typing the following command:

```
mount /store/ariel
```

**d** Remount, in reverse order, the file systems that were unmounted in step**b**.

**Step 6** Verify that your file system is mounted on the external iSCSI device partition by typing the following:

```
df -h
```

The output should resemble the following:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2              19G  4.9G   13G  28% /
/dev/sda3             9.4G  209M  8.7G   3% /var/log
/dev/sda1              94M   13M   77M  15% /boot
tmpfs                 3.9G     0  3.9G   0% /dev/shm
/dev/sdb1              20G  2.6G   17G  14% /store/ariel
/dev/sda5             9.4G  164M  8.8G   2% /store/tmp
```

You are now ready to configure QRadar SIEM to auto-mount the iSCSI volume, see **Reconfigure QRadar SIEM to Auto-mount the iSCSI Volume**.

## Reconfigure QRadar SIEM to Auto-mount the iSCSI Volume

To configure the system to auto-mount the iSCSI volume:

**Step 1** Add the iSCSI script to the startup by typing the following commands:

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

**Step 2** Create a symbolic link to the iscsi-mount script by typing the following command:

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

**Step 3** Add the iscsi-mount script to the startup by typing the following commands:

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

You are now ready to complete the upgrade to QRadar SIEM 7.1, see **Completing the Upgrade to QRadar SIEM 7.1**

## Reconfiguring a Fibre Channel Device

If you migrated /store or /store/ariel to an external Fibre Channel device before upgrading to QRadar SIEM 7.1, you must reconfigure the connections to the Fibre Channel device. After you have you reconfigured the connections you should complete the QRadar SIEM upgrade, see **Completing the Upgrade to QRadar SIEM 7.1**.

**CAUTION**

*Data loss will occur if you reformat the Fibre Channel device partition on which the /store or /store/ariel file system was mounted before upgrading to* QRadar SIEM *7.1.*

This section includes the following topics:

- **Verify that QRadar SIEM is Connected to the Fibre Channel Device**
- **Reconfigure the Fibre Channel Device Mount Points**

### Verify that QRadar SIEM is Connected to the Fibre Channel Device

To verify that QRadar SIEM is connected to the Fibre Channel device:

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

Username: **root**

Password: **<password>**

**Step 2** To verify the attached devices, type the following command:

**dmesg | less**

**Step 3** When the file is open, type the following command to search for the `lpfc` string:

**:/lpfc**

The output may resemble the following:

```
lpfc 0000:06:00.0: 0:1303 Link Up Event x1 received Data: x1 x2
x10 x2 x0 x0 0
Vendor: MAXTOR    Model: ATLAS15K2_146SCA  Rev: JNZ6
Type:   Direct-Access                      ANSI SCSI revision: 03
SCSI device sdb: 286749480 512-byte hdwr sectors (146816 MB)
sdb: Write Protect is off
sdb: Mode Sense: bf 00 10 08
SCSI device sdb: drive cache: write through w/ FUA
SCSI device sdb: 286749480 512-byte hdwr sectors (146816 MB)
sdb: Write Protect is off
sdb: Mode Sense: bf 00 10 08
```

```
SCSI device sdb: drive cache: write through w/ FUA
sdb: sdb1
sd 3:0:0:0: Attached scsi disk sdb
Vendor: MAXTOR    Model: ATLAS15K2_146SCA  Rev: JNZ6
Type:   Direct-Access                      ANSI SCSI revision: 03
```

This example verifies the Fibre Channel link and SCSI drive named sdb is connected to the network.

**NOTE**

A Fibre Channel volume can be connected to QRadar SIEM using a Fibre Channel bridge and a SCSI cable. If this configuration is used, the Fibre Channel volume is identified as a SCSI disk.

### Reconfigure the Fibre Channel Device Mount Points

To configure the Fibre Channel device mount points:

**Step 1** 7Verify the UUID of the Fibre Channel device partition by typing the following command:

**`blkid /dev/<device name>`**

Where **`<device name>`** is the name of the device including the partition number. For example: **`sdb1`**

The output should resemble the following:

```
/dev/sdb1: UUID="89ec181b-dcd1-4698-b1ae-9f1b1b044f62"
```

**Step 2** Reconfigure the /store or /store/ariel mount points using the /etc/fstab file:

**a** Open the fstab file for editing by typing the following command:

**`vi /etc/fstab`**

**b** Add the mount line for the file system that you migrated to the Fibre Channel device before you upgraded QRadar SIEM:

**`UUID=<uuid> <directory> <file system> defaults,noatime,nobarrier 1 2`**

Where:

**`<uuid>`** is the value derived in**Step 1**.

**`<directory>`** is either the /store or store/ariel file system.

**`<file system>`** is the version you used to format the file system.

For example: **`ext4.`**

**c** Save and close the file.

**Step 3** If you migrated the /store file system to the Fibre Channel device before you upgraded QRadar SIEM, go to**Step 4**

If you migrated the /store/ariel file system to the Fibre Channel device before you upgraded QRadar SIEM, go to **Step 5**

**Step 4** Mount the /store file system on the external device partition:

**a** Identify the file systems that should be unmounted before you mount /store by typing the following command:

```
mount | grep ' on /store' | cut -d' ' -f3 | sort -r
```

**b** Unmount each file system in the order they are displayed.

For example: `umount /store/tmp`.

**c** Mount the /store file system by typing the following command:

```
mount /store
```

**d** Remount, in reverse order, the file systems that were unmounted in step **b**.

**Step 5** Mount the /store/ariel file system on the external device partition:

**a** Identify the file systems that should be unmounted before you mount /store/ariel by typing the following command:

```
mount | grep ' on /store/ariel' | cut -d' ' -f3 | sort -r
```

**b** Unmount each file system in the order they are displayed.

**c** Mount the /store/ariel file system by typing the following command:

```
mount /store/ariel
```

**d** Remount, in reverse order, the file systems that were unmounted in step **b**.

**Step 6** Verify that your file system is mounted on the external Fibre Channel device by typing the following command:

```
df -h
```

The output should resemble the following:

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda2   12G 5.4G 6.5G 46% /
/dev/sda1   99M  50M  44M 54% /boot
/dev/sda3   11G 406M 9.7G  4% /var/log
/dev/sdb1  910G 558M 663G  1% /store/ariel
/dev/sda5   10G  33M  10G  1% /store/tmp
```

You are now ready to complete the upgrade to QRadar SIEM 7.1, see **Completing the Upgrade to QRadar SIEM 7.1**

## Reconfiguring an NFS Device

We recommend that you only use a Network File System (NFS) for QRadar SIEM backups, which are stored in the /store/backup/ directory. If you mounted your NFS storage as the /store/backup/ partition, you should reconfigure the connections to the NFS storage device, before completing the QRadar SIEM upgrade. For more information, see **Completing the Upgrade to QRadar SIEM 7.1**.

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

### Reconnect QRadar SIEM to a NFS Device

To reconnect a NFS device:

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

Username: **root**

Password: **<password>**

**Step 2** Open the /etc/hosts file for editing by typing the following command:

```
vi /etc/hosts
```

**Step 3** Add your NFS server to the /etc/hosts file by typing the following line:

```
<IP address> nfsserver
```

Where:

**<IP address>** is the IP address of your NFS server

**Step 4** Save and close the file.

**Step 5** Edit the iptables firewall to allow the connection to your NFS server:

**a** Open the iptables.pre file for editing by typing the following:

```
vi /opt/qradar/conf/iptables.pre
```

**b** Add the following line:

```
-A INPUT -i <interface> -s <IP address> -j ACCEPT
```

Where:

**<interface>** is the QRadar SIEM interface on your NFS network. This is typically

ETH0, unless you have a dedicated NFS network and have connected ETH1 to that network instead of ETH0.

**Step 6** Restart iptables by typing the following command:

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

The NFS services are disaled by default.

**Step 7** Add the NFS to the startup by typing the following commands:

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

**Step 8** Manually start NFS services by typing the following commands:

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

**NOTE**

You might need to adjust the settings on the NFS mount point to accommodate your configuration. For example: **`/nfsshare/qradar/backup /store/backup nfs soft,intr,rw,noac 0 0.`** For more information about common NFS mount options, type **`man nfs`** to view the Unix man page for NFS.

**Step 9** Configure the mount point for /store/backup using the /etc/fstab file:

**a** Open the fstab file for editing by typing the following command:

```
vi /etc/fstab
```

**b** Add the following line:

```
nfsserver:<shared_directory> /store/backup nfs soft,intr,rw 0 0
```

Where:

**`<shared_directory>`** is the path to your shared directory on the NFS server.

**c** Save and close the file.

**Step 10** Remount the /store/backup directory by typing the following command:

```
mount /store/backup
```

**Step 11** Verify that the /store/backup file system is mounted by typing the following command:

```
df -h
```

**Step 12** Verify that your QRadar SIEM backups are stored on the NFS server by typing the following command:

```
ll /store/backup/old
```

You are now ready to complete the upgrade to QRadar SIEM 7.1, see **Completing the Upgrade to QRadar SIEM 7.1**.

## Completing the Upgrade to QRadar SIEM 7.1

You should not complete the upgrade to QRadar SIEM 7.1 until you have reconfigured the connections to your offboard storage devices.

To complete the upgrade to QRadar SIEM 7.1:

**Step 1** Verify that the /store or /store/ariel file system is correctly mounted to the external storage device partition by typing the following command:

```
df -h
```

The output should resemble the following:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2              20G  4.2G   15G  23% /
tmpfs                 4.0G     0  4.0G   0% /dev/shm
/dev/sda1              97M   37M   55M  41% /boot
/dev/sda3             9.4G  2.4G  6.5G  28% /var/log
```

```
/dev/sdb1              20G  1.3G   18G   7% /store
/dev/sda5             9.9G  1.2G  8.3G  12% /store/tmp
```

**Step 2** Complete the upgrade to QRadar SIEM 7.1 by typing the following command:

**/root/complete_upgrade.sh**

The output should resemble the following:

```
Verifying mount points...
Checking recorded mount points: /var/log /store.
OK: All mount points were verified.
```

**Step 3** Verify that the upgrade to QRadar SIEM 7.1 has completed by typing the following command:

**/opt/qradar/bin/myver -v**

The output should resemble the following:

```
Product is 'QRadar'
Appliance is '3100'
Core version is '7.1.0.377154'
Latest version is '7.1.0.377154'
QRM enabled: 'false'
Console: 'true'
Console IP: '172.16.152.112'
IP address: '172.16.152.112'
Vendor: 'Q1 Labs'
Branded Product Name: 'QRadar'
Kernel architecture: 'x86_64'
CPU supports 64bit: 'true'
Operating System: 'Red Hat Enterprise Linux Server release 6.2
(Santiago)'
HA identity: 'N/A'
```

# A NOTICES AND TRADEMARKS

What's in this appendix:



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

## Notices

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive*
*Armonk, NY 10504-1785 U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing*
*Legal and Intellectual Property Law*
*IBM Japan Ltd.*
*19-21, Nihonbashi-Hakozakicho, Chuo-ku*
*Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation*
*170 Tracer Lane,*
*Waltham MA 02451, USA*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http:\\www.ibm.com/legal/copytrade.shtml*.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.