Reconfigure Offboard Storage During a JSA Upgrade

Release 2014.6
Reconfigure Offboard Storage During a JSA Upgrade

Copyright © 2016, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

April 2016 — Reconfigure Offboard Storage During a JSA Upgrade

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html, as modified by the following text, which shall be treated under the EULA as an Entitlement Document taking precedence over any conflicting provisions of such EULA as regards such software:

As regards software accompanying the STRM products (the "Program"), such software contains software licensed by Q1 Labs and is further accompanied by third-party software that is described in the applicable documentation or materials provided by Juniper Networks.
For the convenience of Licensee, the Program may be accompanied by a third party operating system. The operating system is not part of the Program, and is licensed directly by the operating system provider (e.g., Red Hat Inc., Novell Inc., etc.) to Licensee. Neither Juniper Networks nor Q1 Labs is a party to the license between Licensee and the third party operating system provider, and the Program includes the third party operating system “AS IS”, without representation or warranty, express or implied, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement. For an installed Red Hat operating system, see the license file: /usr/share/doc/redhat-release-server-6Server/EULA.

By downloading, installing or using such software, you agree to the terms and conditions of that EULA as so modified.
1 RECONFIGURE OFFBOARD STORAGE DURING A JSA UPGRADE

Removing References to the /store_old File System ......................... 7
Reconfigure an iSCSI Device .................................................... 8
  Reconnecting JSA to the iSCSI Network .................................... 8
  Assigning and Configuring the iSCSI Volumes ............................ 9
  Reconfiguring the iSCSI Device Mount Points ............................ 9
  Reconfiguring JSA to Auto-mount the iSCSI Volume .................... 11
Reconfigure an NFS Device ....................................................... 11
  Reconnecting JSA to a NFS Device ......................................... 12
Completing the Upgrade to JSA 2014.6 ........................................ 14
RECONFIGURE OFFBOARD STORAGE DURING A JSA UPGRADE

This technical note provides information about how to reconfigure iSCSI and NFS storage devices and complete the upgrade to Juniper Secure Analytics (JSA) 2014.6.

CAUTION
Connections and configurations to your offboard storage devices are not maintained when you upgrade to JSA 2014.6.

During the upgrade, you are prompted to reconfigure your offboard storage devices. Ensure that you reconfigure the connections to your devices before you complete the upgrade. For more information about completing the upgrade, see Completing the Upgrade to JSA 2014.6.

Unless otherwise noted, all references to JSA refer to JSA and Log Manager. References to flows do not apply to Log Manager.

Removing References to the /store_old File System

During the JSA 2014.6 upgrade, you might be required to remove references to the /store_old file system.

About this task
If you migrated the /store file system to an external iSCSI device by using JSA 2014.6, the upgrade might prompt you to mount the /store_old directory. Remove references to the /store_old file system.

Procedure

Step 1 Using SSH, log in to the JSA console as the root user.
   Username: root
   Password:<password>

Step 2 Edit the /mounts file by typing the following command:
   vi /tmp/restore_run_state/mounts

Step 3 Remove the line /store_old.
Reconfigure Offboard Storage During a JSA Upgrade

Step 4  Save and close the file.

What to do next
Perform the steps in the procedure, Reconfigure an iSCSI Device.

Reconfigure an iSCSI Device
You must reconfigure the connections to your iSCSI device if you migrated the /store or /store/ariel file system.

! CAUTION
To prevent data loss, never reformat the iSCSI device partition before you upgrade to JSA 2014.6.

To reconfigure your iSCSI device connections, you must:
1  Configure your system to identify the iSCSI device volume. For more information, see Reconnecting JSA to the iSCSI Network.
2  Detect the iSCSI volumes and verify your log in to the iSCSI server. For more information, see Assigning and Configuring the iSCSI Volumes.
3  Reconfigure the iSCSI device mount points. For more information, see Reconfiguring the iSCSI Device Mount Points.
4  Configure JSA to auto-mount the iSCSI volume. For more information, see Reconfiguring JSA to Auto-mount the iSCSI Volume.

Reconnecting JSA to the iSCSI Network
Prepare JSA to connect to your iSCSI network.

Procedure

Step 1  Using SSH, log in to the JSA 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 by typing the following command:
    vi /etc/iscsi/initiatorname.iscsi
  b  Edit the file by typing the following command:
    InitiatorName=iqn.<yyyy-mm>.{reversed domain name}:<hostname>
    For example:
    InitiatorName=iqn.2008-11.com.q1labs:p113
  c  Save and close the file.
Reconfigure Offboard Storage During a JSA Upgrade

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

```
service iscsi restart
```

What to do next
Perform the steps in the procedure, Assigning and Configuring the iSCSI Volumes.

Assigning and Configuring the iSCSI Volumes

Detect the volumes on the iSCSI server.

Before you begin
Perform the steps in the procedure, Reconnecting JSA to the iSCSI Network.

Procedure

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

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

Where:

- `<IP address>` is the IP address of the iSCSI server.
- `<port>` Optional. The port number of the iSCSI server.

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

```
iscsiadm --mode node --login
```

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"
```

What to do next
Perform the steps in the procedure, Reconfiguring the iSCSI Device Mount Points.

Reconfiguring the iSCSI Device Mount Points

Reconfigure the iSCSI device mount points.

Before you begin
Perform the steps in the procedure, Assigning and Configuring the iSCSI Volumes.
To reconfigure your iSCSI 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.

Procedure

**Step 1** 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 iSCSI device partition. For example: `sdb1`

**Step 2** Reconfigure the /store or /store/ariel mount points by using the /etc/fstab file:
   a. Open the fstab file by typing the following command:
       ```
       vi /etc/fstab
       ```
   b. Add the following mount line for the file system that you migrated to the iSCSI device before the JSA upgrade:
       ```
       UUID=<uuid> <directory> <file system>
       noatime,noauto,nobARRIER 0 0
       ```
       Where:
       - `<uuid>` is the value that is derived in **Step 1**.
       - `<directory>` is either the /store or store/ariel file system.
       - `<file system>` is the version that 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 JSA, go to **Step 4**.
   If you migrated the /store/ariel file system to the iSCSI device before you upgraded JSA, go to **Step 5**.

**Step 4** Mount the /store file system on the iscsi device partition:
   a. Identify the file systems that must 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**.

Reconfigure Offboard Storage During a JSA Upgrade
Step 5  Mount the /store/ariel file system on the iscsi device partition:

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

   ```bash
   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:

   ```bash
   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 command:

   ```bash
   df -h
   ```

What to do next
Perform the steps in the procedure, Reconfiguring JSA to Auto-mount the iSCSI Volume.

Reconfiguring JSA to Auto-mount the iSCSI Volume  Reconfigure JSA to auto-mount the iSCSI volume.

Before you begin
Perform the steps in the procedure, Reconfiguring the iSCSI Device Mount Points.

Procedure

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

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

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

   ```bash
   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:

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

What to do next
Perform the steps in the procedure, Completing the Upgrade to JSA 2014.6.

Reconfigure an NFS Device  Use a Network File System (NFS) for JSA backups which are stored in the /store/backup/ directory.

If you mounted your NFS storage as the /store/backup/ partition, then you need to reconfigure the connections to the NFS storage device before completing the JSA upgrade. For more information, see Completing the Upgrade to JSA 2014.6.
For more information about backing up your JSA data, see the Administration Guide for your product.

**Reconnecting JSA to a NFS Device**

Reconnect JSA to a NFS storage device.

Procedure

**Step 1** Using SSH, log in to the JSA console as the root user:

Username: root
Password: <password>

**Step 2** Open the /etc/hosts file 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 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 JSA interface on your NFS network.

**NOTE**

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 disabled 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 nfsslock on
```

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

```
service nfsslock start
service nfs start
```
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 JSA backups are stored on the NFS server by typing the following command:

`ll /store/backup/old`

**What to do next**

Perform the steps in the procedure, **Completing the Upgrade to JSA 2014.6**.
Completing the Upgrade to JSA 2014.6

Complete the upgrade to JSA 2014.6.

About this task

CAUTION

Do not complete the upgrade to JSA 2014.6 until you have reconfigured the connections to your offboard storage devices.

Procedure

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

Step 2  Complete the upgrade to JSA 2014.6 by typing the following command:
        /root/complete_upgrade.sh

Step 3  Verify that the upgrade to JSA 2014.6 has completed by typing the following command:
        /opt/qradar/bin/myver -v