# Quantum®

# StorNext 7.x Xcellis Workflow Extender Release Notes

## Contents

# Revision History

The following StorNext Releases are supported by these Release Notes:

| StorNext 7 Releases Supported | Release Notes Date |
| --- | --- |
| StorNext 7.1.1 | June 2023 |
| StorNext 7.1 | January 2023 |
| StorNext 7.0.3 | June 2022 |
| StorNext 7.0.2 | December 2021 |
| StorNext 7.0.1 | December 2020 |

# About the Xcellis Workflow Extender System

The Xcellis Workflow Extender systems combine industry-proven Quantum hardware and StorNext software into one convenient, out-of-the-box gateway solution. The Xcellis Workflow Extender operates as a SAN Client in a StorNext Metadata Network, providing LAN client access to the StorNext disk SAN. It also can provide NFS and SMB NAS access using StorNext NAS software.

# Training and Documentation Resources

Xcellis Workflow Extender (Gen 2) training and documentation

If you are unsure about which type of system you have visit the "Identify My System" page to determine which system you have, and to find the training and documentation resources for that specific system.

# Learn more about StorNext 7.x

## What is StorNext?

StorNext® is high-performance, multi-tier shared storage designed for large, data-intensive workloads. It includes Xcellis workflow storage, extended online storage, and tape archives—all powered by StorNext, the industry's fastest streaming file system and policy-driven data management software.

At the core of all Quantum scale-out storage is StorNext advanced data management—engineered to tackle the world's most demanding workloads, with the performance and efficiency needed to cost-effectively achieve desired business results.

StorNext 6 delivers the unique combination of high performance and advanced data management, providing cost-effective scalability and access for a wide variety of workloads and use cases, including media production, genomics research, video surveillance, geospatial imaging, VR content, and more.

## Learn More on the Web...

Learn more about StorNext 7 and Scale-Out Storage and take a look at the StorNext 7 Documentation Center, which includes training and documentation resources for StorNext 7, including StorNext software Release Notes.

# What StorNext Releases are compatible with my system?

See the "StorNext Upgrade Matrix" and "StorNext Appliance Compatibility" sections of the StorNext 7.x Compatibility Guide on quantum.com for information about system compatibility.

# Upgrade StorNext Software and System Firmware

Before upgrading your system, refer to Known Issues on page 11. This section contains important information you need to know before upgrading.

See [Upgrade the System (Upgrade Firmware)](#) for the steps necessary to upgrade to the latest StorNext release and hardware firmware for your system.

# General Notes

Refer to the [General Notes](#) page on quantum.com for important information you should know about your system.

# Enhancements, Fixed Issues, and Notes

This section lists the fixed issues, enhancements and notes for different StorNext Releases supported for your system.

- [Enhancements and Fixed Issues for StorNext 7.1.1 below](#)
- [Enhancements and Fixed Issues for StorNext 7.1 on the next page](#)
- [Fixed Issuesfor StorNext 7.0.3 on page 6](#)
- [Enhancements and Fixed Issues for StorNext 7.0.2 on page 7](#)
- [Enhancements and Fixed Issues for StorNext 7.0.1 on page 9](#)

## Enhancements and Fixed Issues for StorNext 7.1.1

**Enhancements:**

- As of StorNext 7.1.1, the Dell/Nvidia Connect X-6 Dual-Port 10/40/25/50/100 GbE Eth NIC card is now supported for Xcellis Workflow Extender (Gen 2) systems.

  > ℹ️ **Note:** The Connect X-6 card requires StorNext 7.1.1 to operate, so the system must first be updated to 7.1.1 before installing and configuring this card.

**Fixed Issues:**

| CR Number | SR Number(s) | Description |
| --- | --- | --- |
| SNXT-112 | 680637 | `netcfg` now correctly identifies available IP addresses. |
| SNXT-114 | n/a | Support added for the Dell/Nvidia Connect X-6 card for Xcellis Workflow Extender (Gen 2) systems **ONLY**. |

| CR Number | SR Number(s) | Description |
| --- | --- | --- |
| SNXT-116 | n/a | `confignetdef.sh` no longer creates a bond1 profile (ifcfg file) with an incorrect DEVICE entry. |
| SNXT-334 | n/a | Updated `tzdata` and `tzdata-java` RPMs to the latest available to account for recent daylight saving changes. |

- See the StorNext 7.1.1 Release Notes for information about StorNext software updates for this release.

- See the "**StorNext Software Compatibility**" section of the StorNext 7.x Compatibility Guide for supported appliances.

- See the Upgrade the System (Upgrade Firmware) for the instructions for upgrading system firmware.

## Enhancements and Fixed Issues for StorNext 7.1

**Enhancements:**

- As of the StorNext 7.1 release, Quantum H2000 and F2100 storage is now supported for metadata (metadata and HAFS), and combo (metadata, HAFS, and data) storage configurations for Xcellis Workflow Director systems.

- For Xcellis Workflow Director (Gen 2) systems, within the next few months, the server used in these systems will no longer be shipped with a PERC RAID card installed. For systems without the PERC card, a software RAID is used instead. This release adds support for the software RAID used in those systems.

**Fixed Issues:**

| CR Number | SR Number(s) | Description |
| --- | --- | --- |
| 80416 | n/a | StorNext upgrades update R640 BIOS firmware to 2.15.1 for new security fixes |
| 80550 | n/a | StorNext no longer issues RAS messages for omcliproxy core failures |
| 80446 | 680010 | Nessus flagged PHP on ports 416, 441 and 442 as vulnerable for 4 newest CVEs - Upgrade php to 7.4.31 |
| 80289 | 671453 | The pre-upgrade check ignores http_proxy settings and completes successfully |
| 80276 | 668727 | The pre-upgrade check provides vaild error messages when it fails, even when the root file system is running low on available space |

| CR Number | SR Number(s) | Description |
|---|---|---|
| 80086 | 663515 | Fix for an issue identified during a Qualys security scan - CentOS Security Update for Open Secure Sockets Layer (OpenSSL) |
| 80061 | n/a | Upgraded Nessus PHP from 7.4.x to 7.4.25 . |
| 79952 | 651056 | On the pre-upgrade check, if a firmware bundle (fw_bundle) version mismatch shows that the firmware installed is newer than the firmware expected, the message is now "INFORMATIONAL" rather than being listed as a "WARNING" <br><br> Example of a 7.1 firmware mismatch message: <br><br> ```INFORMATIONAL: Dell iDRAC9/Life Cycle Controller - iDRAC Information, iDRAC Firmware Information,Firmware Version: Mismatch; Expected: 'lower', Found: higher'``` |
| 79518 | 638473 | For StorNext upgrades, we now verify the md5 checksum file for both .fw files and warn about the image file not matching. We no longer support beginning the upgrade if one of the files does not match the checksum it is validated against. |
| 78885 | 610068 <br> 628424 | Replacement 1TB drives are now rebuilt correctly on Xcellis R640 systems. |

- See the StorNext 7.1 Release Notes for information about StorNext software updates for this release.
- See the "**StorNext Software Compatibility**" section of the StorNext 7.x Compatibility Guide for supported appliances.
- See the Upgrade the System (Upgrade Firmware) for the instructions for upgrading system firmware.

## Fixed Issuesfor StorNext 7.0.3

**Fixed Issues:**

| CR Number | SR Number(s) | Description |
|---|---|---|
| 79783 | n/a | In the **/etc/multipath.conf** file included with 7.0.3, the entries for all devices using **rr_min_io** have been changed to **rr_min_io_rq**. |

| CR Number | SR Number(s) | Description |
|---|---|---|
| 79890 | n/a | After an upgrade to 7.0.2 and Appliance Controller 3.1.0, during an iSCSI conversion from v2 to v3, the MDC could SMITH itself. This is longer a problem after upgrading to 7.0.3 and Appliance Controller 3.1.1. |
| 79976 | 652793 | Firmware bundles missing from the 7.0.2 upgrade are now included in the upgrade files for 7.0.3. |
| 80006 | 631455 | The `qxsarray` utility in the Appliance Controller CLI now uses https for secure data transfer rather than as plain text. |

- See the StorNext 7.0.3 Release Notes for information about StorNext software updates for this release.

- See the "**StorNext Software Compatibility**" section of the StorNext 7.x Compatibility Guide for supported appliances.

- See the Upgrade the System (Upgrade Firmware) for the instructions for upgrading system firmware.

# Enhancements and Fixed Issues for StorNext 7.0.2

**Enhancements:**

- Upgraded the appliance operating system to CentOS 7.9

**Fixed Issues:**

| CR Number | SR Number(s) | Description |
|---|---|---|
| 79607 | N/A | Xcellis Workflow Extender: Setting `mtu=jumbo` in setting of `iscsiadm` now correctly configures interfaces correctly as jumbo frames. |
| 79350 | N/A | Mellanox InfiniBand drivers now correctly identify Mellanox cards after MLNX_OFED installation. |
| 79317 | N/A | The `MLNX_OFED_LINUX LTS` versions have been updated to include support for ConnectX-3 cards. |
| 79300 | N/A | The **Infiniband Service Menu** no longer uses the `connectx_port_config` command since it's no longer supported in new `MLNX_OFED_LINUX` package. |
| 79275 | 612947, 612900 | To avoid lengthy database shutdowns during upgrades, in 7.0.2 we now check the installed `MySQL` version. A script is now installed which determines if a `MySQL` clean shutdown should performed before upgrading. |

| CR Number | SR Number(s) | Description |
|-----------|--------------|-------------|
| 79273 | 618931 | Consistency checks have been added into StorNext appliance software to assist with drive failures. |
| 79254 | N/A | R640 hardware - updated iDRAC firmware to v4.22.00.53 to address a security issue in v4.40.00.00 and later iDRAC firmware. |
| 79181 | 616975 | The **collect_snconnect routine** in **collect-local** now creates snapshots which no longer include prior snapshots and dset output in **/usr/adic/HAM/shared/capture_state**, making for significantly smaller capture log files. <br><br> ⓘ **Note:** This change requires an update to the latest StorNext Connect release. |
| 79126 | N/A | iDRAC/IPMI password requirements have changed for R640 appliances. On a system reboot, you will see an admin alert indicating that the IPMI remote password needs to be changed. <br><br> To change the IPMI remote password, see: https://qsupport.quantum.com/kb/Flare/Content/appliances/ChangeiDRAC.htm |
| 79052 | 612947, 612900 | Upgrades to StorNext 7.0.1 took many more hours longer than previous upgrades to shut down the MySQL database. This is fixed for 7.0.2 and is no longer an issue. |
| 78835 | N/A | Modified firmware install scripts to handle both .BIN and .EXE files. |
| 78663 | N/A | Removed unused packages previously installed with NAS. This includes: cups, cups-filesystem, cups-filters, cups-filters-libs, ghostscript, ghostscript-cups, ghostscript-fonts, java-1.8.0-openjdk, and xorg-x11-fonts-Type1. |
| 76153 | * Multiple SRs addressed. See below | Qualys scans have been completed for 7.0.2. |

* 443251,443252,443253,443254,443255,443256,443258,443259,443260,443261,609514, 443251,443252,443253,443254,443255,443256,443258,443259,443260,443261

- See the StorNext 7.0.2 Release Notes for information about StorNext software updates for this release.

- See the "**StorNext Software Compatibility**" section of the StorNext 7.x Compatibility Guide for supported appliances.

- See the Upgrade the System (Upgrade Firmware) for the instructions for upgrading system firmware.

## Enhancements and Fixed Issues for StorNext 7.0.1

**Enhancements:**

- Upgraded the appliance operating system to CentOS 7.7

**Fixed Issues:**

| CR Number | SR Number(s) | Description |
| --- | --- | --- |
| 78030 | N/A | Updated the FlexSync software to 2.2.1. |
| 77951 | N/A | Updated the Appliance Controller software to 3.0.1. |
| 77884 | N/A | Updated the CBA (computer-based analytics) StorNext Appliance Agent to 2585. |
| 77407 | N/A | Support for the QLogic 2772 FC HBA has been added. This card replaces the QLogic 2742 FC HBA. |
| 77357 | N/A | Added the fcoe-utils RPM (which includes the fcc.sh tool for troubleshooting Fibre Channel issues from the RHEL "fcoe-utils" package) to the StorNext 7.0.1 appliance software. |
| 77326 | N/A | Updated iDRAC firmware to address safety issues in previous iDRAC firmware. |
| 77110 | N/A | Updated default iscsi initiator tuning configuration in the `iscsid.conf` file. |
| 77096 | N/A | Updated the **/etc/multipath.conf** file to include additional Quantum hardware, such as FSeries storage arrays. |
| 76834 | N/A | Updated the OpenManage Server Administrator (OMSA) agent from 9.2.0 to 9.4.0. |
| 76743 | N/A | Remove the Object Store (SWIFT stack) from StorNext 7.0.1 appliance software and the Appliance Controller. |
| 76688 | N/A | Set the permitted/supported software upgrade paths for StorNext 7.0.1 appliance software. |

| CR Number | SR Number(s) | Description |
|---|---|---|
| 76685 | 545545 | Fixed an issue where enabling the SNMP stornext agent (dsm_sa_snmpd) could cause the agent to be stopped, which, as a result, would cause the server node's hardware status to be reported as unknown(Red) in the StorNext GUI under **Reports > Hardware Status**. |
| 76539 | N/A | Updated Moilla Firefox shipped in CentOS7 to 68.4.1-1. |
| 75963 | N/A | Updated Java from JRE 1.8.0.192-1 to the open JDK 1.8.0_242 version included in CentOS7. |
| 75926 | N/A | Updated the StorNext 7.0.1 appliance software to include the **lldpad** utility. |
| 75835 | N/A | Updated the StorNext 7.0.1 appliance software to include the **fio** (Flexible I/O Tester) RPM included in CentOS7. |
| 75726 | 544346 | Operating system software has been upgraded to CentOS 7.7. |
| 74930 | 520303, 556391 | When the system is upgraded to StorNext 7.0.1, it no longer exports **/usr/cvfs/CLIENTS**. |
| 74811 | N/A | StorNext RPMs with Intel MDS security fixes have been updated for StorNext 7.0.1 appliance software. |
| 73126 | N/A | StorNext 7.0.1 appliance software updates have been implemented to address CVE-1999-0514 Fraggle UDP attacks. |

- See the StorNext 7.0.1 Release Notes for information about StorNext software updates for this release.

- See the "**StorNext Software Compatibility**" section of the StorNext 7.x Compatibility Guide for supported appliances.

- See the Upgrade the System (Upgrade Firmware) for the instructions for upgrading system firmware.

# Known Issues

This section lists the known issues that could potentially affect your system.

| CR Number | Customer SR Number | Description |
|---|---|---|
| SNXT-389 | N/A | The StorNext rpm database can become corrupted if an rpm operation or a query is unexpectedly interrupted by a signal, reboot, or a system crash on StorNext NAS-clustered systems or the Unified User Interface (UUI) software runs. |

Querying the database might result in errors and report that an installed package is not installed.

**Example:**

```
$ rpm -q snfs-server
error: rpmdb: BDB0113
Thread/process7492/140149665155136 failed: BDB1507
Thread died in Berkeley DB library
error: db5 error(-30973) from dbenv->failchk:BDB0087
DB_RUNRECOVERY: Fatal error, run databaserecovery
error: cannot open Packages index using db5 - (-
30973)
error: cannot open Packages database in /var/lib/rpm
error: rpmdb: BDB0113
Thread/process7492/140149665155136 failed: BDB1507
Thread died inBerkeley DB library
error: db5 error(-30973) from dbenv->failchk:BDB0087
DB_RUNRECOVERY: Fatal error, run databaserecovery
error: cannot open Packages database in /var/lib/rpm
package snfs-server is not installed
```

These query errors could result in the inability to start StorNext or other Quantum services.

On rare occasions, you might see corruption of the rpm database after are boot of the system while an rpm activity occurred. StorNext, StorNext NAS, and the UUI invoke periodic rpm queries that could be running when a reboot occurs that could lead to corruption. The rpm database corruption is more likely to be seen in the event of an ungraceful reboot resulting from a kernel panic, power outage, or SMITH reset, or upon sending the kill signal to a running rpm command which can happen via systemd as part of a normal shutdown/reboot sequence.

**Workaround:**

1. Log in to the command line of a server node.

2. Run the following command to repair the rpm database:

```
rpmdb --rebuilddb
```

| CR Number | Customer SR Number | Description |
|---|---|---|
| | | 3. After you rebuild the database, run the following query: <br><br> ```rpm -q snfs-server``` <br><br> The server version will be displayed, which verifies the database has been repaired: <br><br> ```snfs-server-7.1.1-91E.RedHat7.x86_64``` |
| SNXT-118 | N/A | **confignetdef.sh** incorrectly creates a bond1 profile in the **ifcfg** file with an incorrect DEVICE entry. <br><br> You may see an error like the following: <br><br> ```2023-01-18-09:13:46.244095 leo kernel: CVFS: Cannot get IP address of NIC with MAC 24-6e-96-a2-a2-59 error "Not found" (2``` <br><br> **Workaround:** <br><br> This issue has been fixed in StorNext 7.1.1. See [SNXT-116](#) in the 7.1.1 Fixed Issues. <br><br> To fix this issue on StorNext prior to 7.1.1, open the **/etc/sysconfig/network-scripts/ifcfg-bond1** file. In the in first line of the file, change the following entry: <br><br> ```DEVICE=bond0:2``` <br><br> to: <br><br> ```DEVICE=bond1:2``` |

| CR Number | Customer SR Number | Description |
|---|---|---|
| 80650 | N/A | If Bond 1 (typically configured with port em2) is not configured during initial system configuration the system can apply settings to Bond 1 which cause the `cvfs` file system to not mount. If you check, the following error will be included in the `/var/log/messages` file:<br><br>```<br>2023-01-18-09:13:46.244095 leo kernel: CVFS: Cannot get IP address of NIC with MAC 24-6e-96-a2-a2-59 error 'Not found' (2)<br>```<br><br>**Workaround:**<br><br>To fix this issue, see 80650 Workaround: Fix the Bond 1 configuration |
| 80640 | N/A | Applies to Xcellis Workflow Director (Gen2/R630), Xcellis Foundation, Artico (R630), and Xcellis Workflow Extender (Gen2/R630) systems.<br><br>On systems reinstalled from ISO or if a Mellanox Connect CX3 card is installed after initial system configuration, DNS configuration settings are removed during the ISO rebuild or after the card is added, causing DNS resolution to fail.<br><br>**Workaround:**<br><br>If DNS resolution fails on your system, you will need to reconfigure StorNext DNS server settings. See 80640 Workaround: Configure missing DNS settings. |
| 80637 | N/A | In some rare occasions upgrades to the Appliance Controller might report an upgrade failure even if the upgrade was successful. To validate if the upgrade failure is a false positive look for this message in the controller log:<br><br>```<br>server.py:142 Appliance controller Failed: local variable 'pid_list' referenced before assignment<br>```<br><br>**Workaround:**<br><br>To resolve this issue, see 80637 Workaround: Appliance Controller upgraded but indicates it did not. |

| CR Number | Customer SR Number | Description |
|---|---|---|
| 80541 | | The appliance StorNext upgrade can report errors and BIOS and iDRAC mismatch errors during the upgrade. |
| | | **Workaround:** |
| | | If this issue is seen, reboot the iDRAC. See 80541 Workaround: Reboot iDRAC on page 22. Then attempt to upgrade the system again. |
| 80393 | 676195 | A RAS ticket may be displayed in the StorNext GUI that indicates an omcliproxy segfault error happened while an IPv6 is bounced on server node , especially when workload on the system is high. |
| | | **Workaround:** |
| | | A workaround for this issue is being investigated. For now, since the omcliproxy utility error message is benign, it can be ignored, and the core file can be deleted. |
| 79052 | 612947, 612900 | The following applies to and systems **ONLY**. It does not apply to other server model names/generations. |
| | | Upgrades to StorNext 7.0.1 may take many more hours longer than previous upgrades. It can take several hours to shut down the MySQL database. If the upgrade is taking an unusually long time, this database issue is most likely affecting the delay. |
| | | ⚠ **Caution: DO NOT** attempt to shut down or reboot the server nodes if the upgrade is taking a long time. |
| | | ℹ **Note:** This was fixed in StorNext 7.0.2, so any upgrades directly to 7.0.2 without first upgrading to 7.0.1 will not experience this issue. |
| | | **Workaround:** |
| | | There is no workaround for this for StorNext 7.0.1. To speed up the MySQL database conversion, upgrade to StorNext 7.0.2 or later and skip the upgrade to 7.0.1, if possible. |
| 74202, 67955, HYDRA-4326 | N/A | If NAS is configured on the system and StorNext services are stopped, StorNext services can fail to stop completely. This can block server fail-over and potentially leaves managed file systems without running FSMs. |
| | | See 74202 – StorNext services can fail to stop completely when NAS is Configured and StorNext services are stopped on page 30 for an in-depth explanation of the issue and several alternate workarounds. |

| CR Number | Customer SR Number | Description |
|---|---|---|
| 73688 | N/A | When the **/var** directory on the appliance gets full, the following serious errors can occur:<br><br>• Network communication errors on the server node<br><br>• iDRAC is not accessible<br><br>• The server node gets stuck during reboot and require a physical power cycle<br><br>See also Leave Space on Appliance File Systems on the *Appliance InfoHub*.<br><br>**Workaround:**<br><br>Keep additional space available on **/var**. |
| 70067 | N/A | **Issue:**<br><br>CentOS 7 systems display log files with the **journalctl** command. Any commands executed as the rootsh user are logged to the system log file . A syslog filter sends all rootsh log commands to /var/log/rootshell. This causes excessive information to be captured in the journalctl log file, and makes the log file difficult to read.<br><br>**Workaround:**<br><br>There is a script to use which removes unnecessary command line output from the syslog file for CentOS7 systems running StorNext 6.0.5 or later:<br><br>See the journalctl Filter Script<br><br>For StorNext releases prior to 6.0.5, contact Contacting Quantum on page 40 and refer to **TSB 2998**. |
| 55318 | N/A | **Issue:**<br><br>Strange UID on ACL when file created on non ads client.<br><br>**Workaround:**<br><br>All systems accessing the StorNext SAN or LAN clients, or the NAS clients, must be part of the same identity domain. Accessing StorNext from different identity domains can result in inconsistent file ownership attributes, as well as potential access problems. |

## 80650 Workaround: Fix the Bond 1 configuration

1. Log in to the CLI:

    a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

**Service Port IP address:**

- 10.17.21.1

b. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: `stornext`
- Password: `<stornext user account password>`

  > **Note:** "`password`" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter `sudo rootsh` to gain root user access.

c. Enter the password for the `stornext` user account again.

2. Manually change the first line of the `/etc/sysconfig/network-scripts/ifcfg-bond1` file from `DEVICE=bond0:2` to `DEVICE=bond1:2`.

The `vi` editor is included in CentOS installed on your system. The following Google search link provides links for editing with `vi`:

https://www.google.com/search?q=edit+with+vi

> **Note:** When finished making changes with the `vi` editor, save and exit the file using `:wq!`.

# 80640 Workaround: Configure missing DNS settings

Configure your DNS settings:

1. Log in to the CLI:

a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

**Service Port IP address:**

- 10.17.21.1

b. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: `stornext`

- Password: `<stornext user account password>`

  > **Note:** "`password`" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter `sudo rootsh` to gain root user access.

c. Enter the password for the `stornext` user account again.

2. Open the **Service Menu**:

a. Launch the **Service Menu**. Enter:

```
sh /opt/DXi/scripts/service.sh -admin
```

The **Service Menu** displays.

3. Navigate to `More Tools > Engineering Tools > Base OS Network Setup > Configure host settings`.

4. Click `<ENTER>` for **Hostname**.

5. Click `<ENTER>` for **Default Gateway IP**.

6. Enter the **Domain Name**,default will show the node name, so replace `node-1` or `node-2` (the system defaults) with a valid domain name to use.

7. Enter one or more (comma-separated) `DNS IP` addresses for the system.

Once you press `<ENTER>`, you should see the settings apply similar to:

```
INFO: *** script started with arguments: addhost --hostname myhostname1 --
domain mydomain.local --dns 10.20.219.63 --defaultgateway
10.20.216.1,10.20.216.2 ***
INFO: *** script completed successfully ***
```

The **Network Menu** displays again.

8. Select the `Activate Network Changes` option to apply the DNS changes.

9. Close the SSH session for this server node.

For single-server node systems, the DNS settings change is now complete.

For dual-server node systems, continue to the next step.

10. Log in to the CLI for the other server node:

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

      **Service Port IP address:**

      - 10.17.21.1

   b. Initiate an ssh session to the system using Terminal or PuTTY:

      **To ssh into the system**

      a. Log in to the command line using the following credentials:

         - User name: **stornext**

         - Password: **`<stornext user account password>`**

           > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

      b. Enter **`sudo rootsh`** to gain root user access.

      c. Enter the password for the **stornext** user account again.

11. Open the **Service Menu**:

   a. Launch the **Service Menu**. Enter:

      ```
      sh /opt/DXi/scripts/service.sh -admin
      ```

      The **Service Menu** displays.

12. Navigate to **`More Tools > Engineering Tools > Base OS Network Setup > Configure host settings`**.

13. Click **`<ENTER>`** for **Hostname**.

14. Click **`<ENTER>`** for **Default Gateway IP**.

15. Enter the **Domain Name**,default will show the node name, so replace **node-1** or **node-2** (the system defaults) with a valid domain name to use.

16. Enter the identical **`DNS IP`** address/addresses entered for the other server node.

17. Once you press `<ENTER>`, you should see the settings apply similar to:

18.
```
INFO: *** script started with arguments: addhost --hostname myhostname1 --
domain mydomain.local --dns 10.20.219.63 --defaultgateway
10.20.216.1,10.20.216.2 ***
INFO: *** script completed successfully ***
```

19. The **Network Menu** displays again.

20. Select the `Activate Network Changes` option to apply the DNS changes.

21. Close the SSH session for this server node.

   For dual-server node systems, the DNS settings change is now complete.

## 80637 Workaround: Appliance Controller upgraded but indicates it did not

1. To determine if the upgrade is incomplete, locate the following error message in the `/var/log/snnas_ controller` log file:

```
server.py:142 Appliance controller Failed: local variable 'pid_ list'
referenced before assignment
```

2. Log in to the server node:

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

   **Service Port IP address:**

   - 10.17.21.1

   b. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: `stornext`

- Password: `<stornext user account password>`

  > **Note:** "`password`" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter `sudo rootsh` to gain root user access.

c. Enter the password for the `stornext` user account again.

3. Verify the Appliance Controller was upgraded and is running the latest/expected release on the current server node:

```
qtmcontroller -c 'system show version'
```

4. If the release is installed as expected. Enter the following on the server node to remove the touch file placed on the system to indicate an upgrade issue on the server node:

```
rm /var/DXi/upgrade_ notify
```

## 80565 Workaround: Restart "docker services" on Node 2

1. Log into the CLI of the server node, if not already logged in.

**How to log into the server CLI:**

a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network.

b. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a.  Log in to the command line using the following credentials:

- User name: `stornext`

- Password: `<stornext user account password>`

    **ⓘ Note:** "`password`" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b.  Enter `sudo rootsh` to gain root user access.

c.  Enter the password for the `stornext` user account again.

2. Enter the docker restart command:

```
systemctl restart docker
```

3. Exit the CLI.
4. Launch the StorNext User Interface again.

# 80541 Workaround: Reboot iDRAC

1. Log in to the server node:

   a.  Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

   **Service Port IP address:**

   - 10.17.21.1

   b.  Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: `stornext`

- Password: `<stornext user account password>`

> **ⓘ Note:** "`password`" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter `sudo rootsh` to gain root user access.

c. Enter the password for the `stornext` user account again.

2. Open the **Service Menu**:

a. Launch the **Service Menu**. Enter:

```
sh /opt/DXi/scripts/service.sh -admin
```

The **Service Menu** displays.

3. Navigate to `Hardware Configuration > Setup IPMI > Configure IPMI`.

4. On the prompt to set to system defaults, enter yes.

5. Confirm setting IPMI to system defaults. The iDRAC/IPMI will reboot.

For single-server node systems, the procedure is complete.

For dual-server node systems:

6. Reboot the iDRAC on the other server node using the steps you just completed on this server node.

# 80334 Workaround: HBA crash and firmware dump files

When you experience this issue, you need to set the `ql2xenabledif_tgt` value to 0 and the `qlport_down_retry` value to 14:

1. Create the /etc/modprobe.d/hpe.conf file. Or, if it exists, create another unique but identifiable file name for this setting)

2. Log in to the server node:

a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network.

b. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: **stornext**

- Password: **<stornext user account password>**

> 🛈 **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter **sudo rootsh** to gain root user access.

c. Enter the password for the **stornext** user account again.

3. Display the contents of the /etc/modprobe.d/hpe.conf file:

```
cat /etc/modprobe.d/hpe.conf
```

It should contain the following entries:

```
options qla2xxx qlport_down_retry=14
options qla2xxx ql2xenabledif_tgt=0
```

If not, add retry and tgt options to the file.

4. If you made changes to the file, save the file.

5. Recreate the **initramfs** with this new information.

> 🛈 **Note:** Do not reboot the system before completing the following 3 steps.

6. Move the img:

```
mv /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.prehpe
```

7. Create the initial image used by the kernel for preloading the block device modules:

> 🛈 **Note:** There are two dashes before **kver** in the following command.

```
dracut --kver $(uname -r)
```

8. Enter the following to set the reboot options that ensure the new **initramfs** file is generated:

```
ls /boot/initramfs-$(uname -r).img
```

9. Reboot the node. Enter:

```
reboot
```

10. After the reboot, verify the **qlport_down_retry** value is now set to **14** as described here:
    **cat /sys/module/qla2xxx/parameters/qlport_down_retry**

# 80181: RAS ticket recommended actions for software RAID failures

1. Log in to the CLI:

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

      **Service Port IP address:**

      - 10.17.21.1

   b. Initiate an ssh session to the system using Terminal or PuTTY:

      **To ssh into the system**

         a. Log in to the command line using the following credentials:

            - User name: **stornext**

            - Password: **<stornext user account password>**

               ℹ **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

         b. Enter **sudo rootsh** to gain root user access.

         c. Enter the password for the **stornext** user account again.

2. Open the **Service Menu**:

a. Launch the **Service Menu**. Enter:

```
sh /opt/DXi/scripts/service.sh -admin
```

The **Service Menu** displays.

3. Navigate to `More Tools > SW RAID Tools`.

4. To repair a software RAID configuration, select the `SW RAID Repair` option.

## 80121 Workaround: Firmware/BIOS fails silently during StorNext upgrade

To check if there was a failure of applying Dell f/w updates, do the following. First, og in to the CLI of the server node that is currently not acting as primary, which prevents a failover if a manual CLI re-install of the StorNext software/reboot is required after the check. We will repeat the steps for the other server node during this process, and upgrade that firmware manually from the CLI, if needed.

1. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

   **Service Port IP address:**

   - 10.17.21.1

2. Initiate an ssh session to the system using Terminal or PuTTY:

   **To ssh into the system**

   a. Log in to the command line using the following credentials:

      - User name: **stornext**

      - Password: **<stornext user account password>**

        > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

3. From the CLI, change to the firmware directory. Enter:

```
cd /opt/DXi/firmware
```

4. From the CLI, run the following command. Enter:

```
./fw_regenall.sh
```

**Example output:**

```
fw_bundle: Performing firmware cleanup.
fw_bundle: Firmware cleanup completed successfully.
fw_bundle: Checking Firmware Bundle Version.
fw_bundle: Need to generate CoR files for the first time.
fw_bundle: Performing firmware CoR generation...
fw_bundle: Firmware CoR generation completed successfully.
fw_bundle: Performing firmware description report.
fw_bundle: Generating firmware description manifests.
fw_bundle: Firmware manifest generation is disabled.
fw_bundle: Generating firmware bundle manifest.
fw_bundle: Firmware manifest generation is disabled.
fw_bundle: Generation of the firmware bundle manifest completed
successfully.

fw_bundle: Performing firmware bundle report.
fw_bundle: Performing TXT firmware report.
fw_bundle: Performing GUI firmware report.
fw_bundle: GUI Firmware reporting completed successfully.
fw_bundle: TXT Firmware reporting completed successfully.
fw_bundle: Firmware reporting completed successfully.
```

At this time, you could check the firmware versions installed by checking the FirmwareReport.txt file. To view the file contents, enter:

```
cat /opt/DXi/hwdetect/FirmwareReport.txt
```

5. From the CLI, run the following command. Enter:

```
./fw_check.sh
```

There are three possible outputs that you may seewhen you run the fw_check.sh command:

- **Example Output #1** - If you see the following message, a firmware **IS NOT** required:

```
fw_bundle: Performing firmware check.
.
.
fw_bundle: Firmware check completed successfully. All firmware is
up-to-date.
```

The firmware check output above shows that the firmware installed on the system is up-to-date. There are no further actions to take. You can exit the **rootsh** session, and close the SSH terminal client.

- **Example Output #2** - If you see the following message, a firmware update **IS NOT** required:

```
fw_bundle: Performing firmware check.
fw_bundle: WARNING: Dell r630 iDRAC8/Life Cycle Controller - iDRAC
Information,
iDRAC Firmware Information, Firmware Version: Mismatch; Expected:
'2.70.70.70',
Found: '2.75.75.75'
fw_bundle: WARNING: Dell r630 BIOS - BIOS Information, BIOS Firmware
Information,
Version: Mismatch; Expected: '2.9.1', Found: '2.11.0'e.
.
.
fw_bundle: WARNING: One or more firmware packages have a mismatched
configuration.
```

The firmware check output above shows that the firmware installed on the system is newer than the firmware included in the StorNext software update. There are no further actions to take. You can exit the **rootsh** session, and close the SSH terminal client.

- **Example Output #3** - If you see the following message, a firmware update **IS** required. The firmware check shows that there is one or more firmware on the system that is older than what is included in the included in the StorNext software update:

```
fw_bundle: Performing firmware check.
fw_bundle: WARNING: Dell r630 iDRAC8/Life Cycle Controller - iDRAC
Information, iDRAC
Firmware Information, Firmware Version: Mismatch; Expected:
'2.70.70.70', Found: '2.75.75.75'
fw_bundle: WARNING: Dell r630 BIOS - BIOS Information, BIOS Firmware
Information, Version:
```

```
Mismatch; Expected: '2.11.0', Found: '2.9.1'.
```

Continue to Step 6.

6. If you need to re-apply the f/w update, run the following command:

```
./fw_install.sh
```

If a server reboot is required, the system will reboot.

7. Exit the **rootsh** session.

8. Exit the SSH terminal session.

9. Repeat Step 1 through Step 8 for the server node acting as primary.

If this does not fix the StorNext Connect issue, contact Quantum Support for assistance.

## 80099 Workaround: Potential StorNext Connect issues after you upgrade StorNext

Do the following to stop and restart StorNext Connect. Log in to the CLI of node 2 **ONLY**, since StorNext Connect does not run on node 1:

1. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

**Service Port IP address:**

- 10.17.21.1

2. Initiate an ssh session to the system using Terminal or PuTTY:

**To ssh into the system**

a. Log in to the command line using the following credentials:

- User name: **stornext**
- Password: **&lt;stornext user account password&gt;**

  **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter **sudo rootsh** to gain root user access.

c. Enter the password for the **stornext** user account again.

3. From the CLI of node 2, stop StorNext Connect. Enter:

```
/opt/quantum/connect/bin/connect stop
```

4. From the CLI of node 2, start StorNext Connect. Enter:

```
/opt/quantum/connect/bin/connect start
```

5. Exit the **rootsh** session.

6. Exit the SSH terminal session.

If this does not fix the StorNext Connect issue, contact Quantum Support for assistance.

## 74202 – StorNext services can fail to stop completely when NAS is Configured and StorNext services are stopped

**How might this be seen?**

There are two basic scenarios where this might be exposed:

### Scenario # 1

When StorNext stops, it signals NAS to vacate the StorNext file systems that NAS is using. However, if these file systems remain available for too long, the Appliance Controller will attempt to automatically restart NAS services. This is what happens, in order:

1. Restarting NAS services can resume use of StorNext resources.

2. Resuming StorNext resources interferes with attempts to stop StorNext.

3. Continued use of these StorNext resources can result in mounted StorNext file systems that do not have a running fsm process which blocks access to the StorNext file system.

If experience this on your system, temporarily stop NAS services:

1. Log in to the command line of the server (as "sudo rootsh"):

   **Launch the Command Line With an SSH Utility**

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management/LAN Client network.

a. Log in to the command line using the following credentials:

- User name: **stornext**

- Password: **<stornext user account password>**

  > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

b. Enter **sudo rootsh** to gain root user access.

c. Enter the password for the **stornext** user account again.

2. Stop NAS by executing the following command:

```
/usr/cvfs/lib/snnas_control stop
```

3. Stop the Appliance Controller by executing the following command:

```
/usr/local/quantum/bin/sml_service_tool stop snnas_controller
```

4. When you have finished Restart NAS and the Appliance Controller:

a. Start NAS by executing the following command:

```
/usr/cvfs/lib/snnas_control start
```

b. Start the Appliance Controller by executing the following command:

```
/usr/local/quantum/bin/sml_service_tool start snnas_controller
```

**Scenario # 2**

If you need to stop the system during a maintenance window. This is an extension of **Scenario #1**, but NAS must vacate the file systems for an extended period of time. If NAS services are resumed when they should be suspended, those service processes may interfere with maintenance operations.

To affect both scenarios, timers exist that you can adjust to extend the amount of time required between the **stornext stop** operation and before NAS services resume. The timers are controlled by the following **Controller Registry** values:

- **nas.heartbeat.check_state_secs**
- **stornext_service.stop_period**

To see what values are currently assigned, enter:

```
su sysadmin -c 'reg show nas.heartbeat.check_state_secs'
```

to display the setting of the frequency interval of the NAS heartbeat state check, or enter:

```
su sysadmin -c 'reg show stornext_service.stop_period'
```

to display the duration that StorNext services are stopped.

> **Note:** By default, both timers are set to 120 (in seconds=2 minutes).

**Workarounds**

**Workaround #1**

If StorNext fails to stop due to NAS resource usage, do the following:

1. Log in to the command line of the server:

   **Launch the Command Line With an SSH Utility**

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management/LAN Client network.

   a. Log in to the command line using the following credentials:

      - User name: **stornext**
      - Password: **<stornext user account password>**

        > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

2. Verify that the StorNext file systems are mounted:

   ```
   grep cvfs /proc/mounts
   ```

If any StorNext file systems are not mounted, mount them now.

3. Mount the HA shared file system:

```
mount /usr/adic/HAM/shared
```

4. Start fsm for each StorNext file system (shown below as "<FSNAME>") mounted on the server node:

```
cvadmin -e "start <FSNAME> on localhost"
```

5. Stop StorNext services:

    For CentOS7 systems, enter:

```
systemctl stop cvfs
```

    For CentOS6 systems, enter:

```
service cvfs stop
```

6. To stop NAS, enter:

```
/usr/cvfs/lib/snnas_control stop
```

7. To stop the Appliance Controller, enter:

```
/usr/local/quantum/bin/sml_service_tool stop snnas_controller
```

    When you are ready, restart the Appliance Controller and NAS services:

8. To restart the Appliance Controller, enter:

```
/usr/local/quantum/bin/sml_service_tool start snnas_controller
```

9. To restart NAS, enter:

```
/usr/cvfs/lib/snnas_control start
```

**Workaround #2**

For **Scenario #1**, Quantum recommends that you extend the time period to a value of 10 minutes (600 seconds) for both variables. Set a value that exceeds the amount of time necessary for typical StorNext shutdown.

To set new values:

1. Log in to the command line:

   **Launch the Command Line With an SSH Utility**

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management/LAN Client network.

   a. Log in to the command line using the following credentials:

   - User name: **stornext**

   - Password: **<stornext user account password>**

     ℹ **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

2. Change the frequency interval of the NAS heartbeat state check to 600 seconds (10 minutes). Enter:

   ```
   su sysadmin -c 'reg set nas.heartbeat.check_state_secs 600'
   ```

   ℹ **Note:** This is run with a temporary log in to the Appliance Controller as the **sysadmin** user.

3. Change the duration that StorNext services are stopped to 600 seconds (10 minutes). Enter:

   ```
   su sysadmin -c 'reg set stornext_service.stop_period 600'
   ```

4. ℹ **Note:** This is run with a temporary log in to the Appliance Controller as the **sysadmin** user.

**Workaround #3**

For **Scenario #2**, to eliminate the confusion of setting a long duration for a maintenance window, and then having to change the values back again to a shorter value again, you can simply stop NAS services and the Appliance Controller, and then restart these services when you are finished.

To stop the services and restart them:

1. Log in to the command line:

   **Launch the Command Line With an SSH Utility**

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management/LAN Client network.

   a. Log in to the command line using the following credentials:

      - User name: **stornext**

      - Password: **<stornext user account password>**

        > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

2. Stop NAS by executing the following command:

   ```
   /usr/cvfs/lib/snnas_control stop
   ```

3. Stop the Appliance Controller by executing the following command:

   ```
   /usr/local/quantum/bin/sml_service_tool stop snnas_controller
   ```

   When you are ready, restart the Appliance Controller and NAS services:

4. To restart the Appliance Controller, enter:

   ```
   /usr/local/quantum/bin/sml_service_tool start snnas_controller
   ```

5. To restart NAS, enter:

```
/usr/cvfs/lib/snnas_control start
```

6. Change the settings for the NAS heartbeat state check and the duration that StorNext services are stopped according to Workaround #2 on page 34.

**Workaround #4**

An alternate method for maintenance windows, instead of implementing workaround #3 for **Scenario #2**, you can choose a much longer value if you need the NAS heartbeat state check interval and StorNext services stopped for a long period of time (for example, during a planned maintenance window in a data center). While this is another option, the downside of this is that you will need to know how much downtime to expect maintenance to take, and then set these times to be less than what is needed for that maintenance. It is also difficult to extend the maintenance period reliably once those timers have started. In addition, you will most likely have to reset the values back to their original settings when the maintenance window is complete, which could be a hassle.

Here is one example which extends the time values to 2 hours (7,200 seconds):

1. Log in to the command line:

   **Launch the Command Line With an SSH Utility**

   a. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management/LAN Client network.

   a. Log in to the command line using the following credentials:

   - User name: **stornext**

   - Password: **<stornext user account password>**

     > **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

2. Change the frequency interval of the NAS heartbeat state check to 7,200 seconds (10 minutes). Enter:

```
su sysadmin -c 'reg set nas.heartbeat.check_state_secs 7200'
```

> **Note:** This is run with a temporary log in to the Appliance Controller as the **sysadmin** user.

3. Change the duration that StorNext services are stopped to 7,200 seconds (10 minutes). Enter:

```
su sysadmin -c 'reg set stornext_service.stop_period 7200'
```

4. ⓘ **Note:** This is run with a temporary log in to the Appliance Controller as the **sysadmin** user.

# journalctl Filter Script

The following applies to Xcellis Workflow Extender (Gen2/R630) supported on CentOS7.

**Step 1: Upgrade to StorNext 6.0.5**

ⓘ **Note:** StorNext 6.0.5 provides the script, so you need to upgrade to StorNext 6.0.5 to access the file.

See Upgrade a Gateway System (Upgrade Firmware) Using the Service Menu.

**Step 2: Log in to the System Command Line**

1. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

   **Service Port IP address:**

   - 10.17.21.1

2. Initiate an ssh session to the system using Terminal or PuTTY:

   **To ssh into the system**

   a. Log in to the command line using the following credentials:

      - User name: **stornext**

      - Password: **<stornext user account password>**

        ⓘ **Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

3. Continue to Step 3: Run the Journal Filter Script and View the Script Help on the next page.

**Step 3: Run the Journal Filter Script and View the Script Help**

- Enter the following to use the script to view the log output in a way that filters out all the `rootsh` commands:

```
/opt/DXi/scripts/journalctl_filter.sh -f
```

- Enter the following to view the script's help file:

```
/opt/DXi/scripts/journalctl_filter.sh --help
```

**ⓘ Note:** The `journalctl_filter.sh` output can also be saved to a file.

# How to Disable NFS v4

To disable NFSv4 on Xcellis Workflow Extender systems, perform the following on the server:

**Edit the nfs File**

1. Open an SSH connection to the appropriate server and use the IP address assigned to the node on the Management or LAN Client network, or use the Service Port IP address.

   **Service Port IP address:**

   - 10.17.21.1

2. Initiate an ssh session to the system using Terminal or PuTTY:

   **To ssh into the system**

   a. Log in to the command line using the following credentials:

      - User name: **stornext**

      - Password: **\<stornext user account password\>**

        **ⓘ Note:** "**password**" is the default password for the stornext user account. If the password has been changed, use the current password. Beginning with StorNext 7.0.2, you must change the default password for the stornext user account. As of StorNext 7.0.2, the first time you log in, you will be prompted to change the password to a different one.

   b. Enter **sudo rootsh** to gain root user access.

   c. Enter the password for the **stornext** user account again.

3. Edit **/etc/sysconfig/nfs** file. (See Example: Use vi to Edit the nfs File on the next page)

4. Change the value for RPCNFSDARGS to "-N 4". When finished, the line must be: RPCNFSDARGS="-N 4"

5. Change the value for RPCMOUNTDOPTS to "-N 4". When finished the line must be: RPCMOUNTDOPTS="-N 4"

6. Save the file.

## Restart NFS (for CentOS7-based Systems)

For Xcellis Workflow Extender (Gen2/R630) systems.

1. Enter the following to restart the NFS configuration.:

```
systemctl restart nfs-config
```

2. Enter the following to restart the NFS server.:

```
systemctl restart nfs-server
```

## Restart NFS (for CentOS6-based Systems)

For Xcellis Workflow Extender (R520) systems.

1. Enter the following to restart the NFS configuration:

```
service nfs-config restart
```

2. Enter the following to restart the NFS server:

```
service nfs-server restart
```

## After You Restart NFS on the Server

**Example: Use vi to Edit the nfs File**

1. Enter the following:

```
vi /etc/sysconfig/nfs
```

2. Move the cursor to the closing quotation mark in RPCNFSDARGS.

3. Enter the following:

```
i -N 4
```

4. Write the file and quit vi as follows:

```
:wq
```

5. For this example, you would have to Restart NFS (for CentOS7-based Systems) on the previous page OR Restart NFS (for CentOS6-based Systems) on the previous page.

6. Close the SSH session for the server .

.

# Quantum Appliance Licenses

See Quantum Appliance Licenses page on quantum.com.

# Contacting Quantum

For further assistance, contact the Quantum Customer Support Center:

| Region | Support Contact |
| --- | --- |
| North America | 1-800-284-5101 (toll free)<br>+1-720-249-5700 |
| EMEA | +800-7826-8888 (toll free)<br>+49 6131 324 185 |

| Region | Support Contact |
|---|---|
| Asia Pacific | +800-7826-8887 (toll free)<br>+603-7953-3010 |

For worldwide support:

https://www.quantum.com/en/company/contact-us/