Sun StorageTek™ NAS OS Software Release Notes

Version 4.21.M2

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6652-20
October 2007, Revision A

Submit comments about this document at: http://www.sun.com/hwdocs/feedback

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.

Contents

New Features in This Release 2

New Features in Previous Release 2

System Requirements 4

Software Updates and Downgrades 5

Service Contact Information 5

Resolved Issues in This Release 6

- NDMP 6
- General 6

Resolved Issues in Previous Release 7

Known Issues 10

- Web Administrator Issues 10
- Copy Issues (`rsync`) 13
- Backup Issues (NDMP) 13
- Antivirus-Specific Issue 14
- Array Firmware-Specific Issues 14
- Cluster-Specific Issues 14
- Sun StorageTek File Replicator Issues 16
- iSCSI-Specific Issues 17
- Documentation Issues 18

Addenda to the Documentation 19

- About the McAfee Secure Internet Gateway 19
- About the `rsync` Protocol 20
- About Online System Registration and Auto Service Request (ASR) 22
- Creating a Core Dump File 24
- Configuring Quotas With Limits 25
- Collecting Information for Configuration 26
- Using a Sun StorageTek Flexline 380 27
- Exempting a Host Group from Virus Scans 28
- Restrictions on Sun StorageTek File Replicator 28
- Upgrading to NDMP V4 28
- Using a Sun StorageTek 5320 NAS Expansion Unit With a Sun StorEdge 5300 RAID EU Controller Enclosure 30
- Using a Sun StorageTek 5320 RAID Controller Unit With a Sun StorEdge 5300 RAID CU Controller Enclosure 30

Release Documentation 36

Sun StorageTek NAS OS Software Release Notes, Version 4.21.M2

These release notes contain information for the Sun StorageTek™ NAS OS, releases 4.21 4.21 Maintenance 1 (4.21.M1) and this release, 4.21 Maintenance 2. The maintenance release resolves issues detected in the previous release.

The Sun StorageTek NAS OS and its options, the StorageTek File Replicator and StorageTek Compliance Archiving Software, manage the following:

- Sun StorageTek 5320 NAS Appliance
- Sun StorageTek 5320 NAS Cluster Appliance
- Sun StorageTek 5320 NAS Gateway System
- Sun StorageTek 5320 NAS Cluster Gateway System
- Sun StorageTek 5220 NAS Appliance
- Sun StorEdge™ 5310 NAS Appliance
- Sun StorEdge 5310 NAS Cluster Appliance
- Sun StorEdge 5310 NAS Gateway System
- Sun StorEdge 5310 NAS Cluster Gateway System
- Sun StorEdge 5210 NAS Appliance

These release notes contain the following sections:

- "New Features in This Release" on page 2
- "New Features in Previous Release" on page 2
- "System Requirements" on page 4
- "Software Updates and Downgrades" on page 5
- "Resolved Issues in This Release" on page 6
- "Resolved Issues in Previous Release" on page 7
- "Known Issues" on page 10
- "Addenda to the Documentation" on page 19
- "Release Documentation" on page 36
- "Service Contact Information" on page 5

New Features in This Release

The following change has been made in this release:

> It is no longer possible to unload the ssh module. This module contains functionality that is required by other parts of the system.(6595606)

New Features in Previous Release

Version 4.21 of the Sun StorageTek NAS operating system (OS) provided the following new features:

- The CIFS service now accepts connections for file sharing from either the SMB-over-NetBIOS or SMB-over-TCP transport layer by listening on both the SMB-over-NetBIOS port 139 and the SMB-over-TCP port 445. The SMB-over-TCP transport layer does not depend on NetBIOS and uses DNS for host name resolution. (RFE 6537850)
- Additional antivirus engine support:
  - McAfee Secure Internet Gateway 3000, 3100, 3200, and 3300 appliances and the Secure Web Gateway 3400 appliances running a minimum of SCM version 4.21 Patch 5 are now supported and can be used in the same way as the other supported scan engine software products. See "About the McAfee Secure Internet Gateway" on page 19.
  - Version 3.1 of the Sun StorageTek 5000 NAS ICAP Server for Computer Associates Antivirus Scan Engine is now available and supported in this release. The document, *Sun StorageTek 5000 NAS ICAP Server for Computer Associates Antivirus Scan Engine* (819-6761-13), has been revised. To use the Computer Associates Antivirus scan engine, use this release and download the ICAP Server for CA package from the Sun Download Center, `http://www.sun.com/download`.
- Support for `rsync`, a protocol that transfers changes to files between a Sun StorageTek 5000 NAS system and a remote system. Use `rsync` for purposes that require more efficiency than the `ftp` protocol and more control than the `rcp` protocol, but do not require a real-time replication solution such as the Sun StorageTek File Replicator option. See "About the `rsync` Protocol" on page 20.
- Enhancements to serviceability:

  - Additional information for the Online System Registration and Auto Service Request (ASR) feature, which enables your NAS appliance or gateway system to report problems and send diagnostic data to Sun Services. See "About Online System Registration and Auto Service Request (ASR)" on page 22.
  - Additional information on creating core dump files. To diagnose some problems, support engineers often request a core dump file. See "Creating a Core Dump File" on page 24.
- The Assured Delete feature provides commercial-grade scrubbing of data on deletion to provide enhanced data security.
- iSCSI robustness enhancements:
  - Red Hat™ iSCSI: Red Hat Enterprise Linux 4 Update 4
  - iSCSI boot
  - Qlogic iSCSI HBA: QLA4052C
- Additional antivirus engine support: Trend Micro™ is now supported.
- CIFS enhancements: The Autohome feature extends the storage capability to home directories.
- Support for Online System Registration and Auto Service Request (ASR) feature, which enables your NAS appliance or gateway system to report problems and send diagnostic data to Sun Services.
- Support for NDMP V4 in addition to V3: Local, remote or three-way backup with supported third-party NDMP-enabled backup products to provide efficient and secure centralized backup and restore implementation with improved reliability.
- Replication enhancement: Both heads in a cluster participate in a replication/mirroring function simultaneously.
- Support for the use of Sun StorageTek 5320 Expansion Units with Sun StorageTek 5300 RAID EU Controller Enclosures. See "Using a Sun StorageTek 5320 NAS Expansion Unit With a Sun StorEdge 5300 RAID EU Controller Enclosure" on page 30.
- Support for the use of Sun StorageTek 5320 RAID Controller Unit with Sun StorageTek 5300 RAID CU Controller Enclosure. See "Using a Sun StorageTek 5320 RAID Controller Unit With a Sun StorEdge 5300 RAID CU Controller Enclosure" on page 30.
- Support for the McData 4400 Director FC Switch for improved SAN connectivity.

System Requirements

The Sun StorageTek NAS OS is pre-installed on all supported platforms. You do not need to install any software to manage the Sun StorageTek 5000 NAS family of products.

To access the Web Administrator management interface, you must have a network-attached computer running one of the following browsers. You must use a Java™ technology-enabled browser with Java Plug-In 1.4.0 (minimum version).

- Internet Explorer
- Mozilla™
- Netscape Navigator™

Note – To download the latest Java Plug-in software, go to http://java.sun.com/javase/downloads/index.jsp.

▼ To Determine the Software Version

Perform one of the following procedures.

- From the Web Administrator navigation panel, select System Operations → Update Software.
- From the console administrator, type the `version` command, as shown in the following example and sample response:

```
hostname> version
StorageTek Model 5320 NAS S/N ST532020051026002 Version 4.21 MO (Build 123)
```

If the appliance is not at the latest release, download and install the release of the Sun StorageTek NAS OS from the SunSolve site, `http://sunsolve.sun.com`.

▼ To Determine Firmware Revision Levels

Use the following command to display the current revision level of the firmware of each RAID controller unit, expansion unit, controller NVSRAM, and drive.

```
raidctl get type=lsi target=profile ctlr=0..N
```

Software Updates and Downgrades

Upgrade your system by downloading the latest release of Sun StorageTek NAS OS software from the SunSolve site, `http://sunsolve.sun.com`. This requires a valid service contract. Select the Patchfinder link, and then enter the patch number that is appropriate for your system.

118216	Software for the Sun StorEdge 5210 Appliance
119351	Software for the Sun StorEdge 5310 Appliance
119352	Software for the Sun StorageTek 5320 or 5220 Appliance

---

Note – If you are upgrading a Sun StorEdge 5210 NAS Appliance to software release 4.21.M1 from a release prior to release 4.05, Field Change Order (FCO) 257 is required. Contact Sun^{SM} Service to get FCO 257 applied prior to upgrading your software. Any Sun StorEdge 5210 NAS Appliance with software release 4.05 (or greater) does not need the FCO applied.

When the software is upgraded, the previous release remains on the system so you can reboot to the previous release. Downgrading to an earlier release other than the one loaded on your system, as indicated on the Shutdown the Server screen of the Web Administrator, is not supported. If required, contact Sun Services.

Service Contact Information

If you need help installing or using this product, call 1-800-USA-4SUN, or go to:

`http://www.sun.com/service/contacting/`

Resolved Issues in This Release

The following issues have been resolved in this release. Change Request numbers are in parentheses.

NDMP

- The NAS appliance no longer appears to hang when attached to a tape library. Information from previous tape backups is now cleared so that the NAS appliance no longer receives failed access requests, resulting in a long boot delay. (6524650)
- Long filenames are now allowed in backup and restore operations. (6592230)
- Using the NAS appliance as a data server but without attached library hardware no longer causes the NAS appliance to crash. (6592583)
- A null session during a backup operation no longer causes the NAS appliance to crash. (6591010).

General

- An NFS request that requires access to a large directory or multiple clients no longer causes the NAS appliance to stall. (6554526/6577456)
- It is now possible to use a short filename (8.3) to get access to a CIFS share. (6573204)

Resolved Issues in Previous Release

The following issues have been resolved with NAS OS release 4.21. Change Request numbers are in parentheses.

- Joining a Windows domain that has an existing (pre-staged) computer account for the NAS appliance is now supported. When creating the account on a Windows 2000 domain controller, select "Allow pre-Windows 2000 computers to use this account". When creating the account on a Windows 2003 domain controller, select "Assign this computer account as a pre-Windows 2000 computer". (6500426)
- SGID-based inheritance now works properly for CIFS clients. (6529924)
- When searching for an ADS server to join the domain, a NAS appliance now searches the ADS domain by default and searches the DNS domain only if the ADS domain does not exist. Previous versions used the DNS domain by default. (6547657)
- The NAS appliance with a FC-connected C4 tape library now recognizes the robot and all tape drives. (6547423)
- Checkpoint age is now determined by individual mapping entries rather than the main entry. The `ls` command for .chkpnt on volume directories can now display accurate results. (6527721)
- The NAS OS can now handle UIDs of up to 10 digits. (6524252)
- Copying files with streams is now supported to improve compatibility with the Brocade StorageX solution. (6565909)
- On Windows systems, it is now possible to delete a quarantined file through a CIFS share. (6539915/649950)
- The NAS appliance can now handle an improper disconnection from a Telnet session. (6550235)
- An invalid rsync command no longer causes a Telnet session to hang. (6551606)
- The backup operations using NDMP have been improved. The current version meets performance requirements set by previous versions (6556386) and restores BakBone NetVault® datasets properly. (6575307 and 6564097)
- Using the product with the StorageTek Flexline™ FLX380 enterprise storage system has been improved. See "About Online System Registration and Auto Service Request (ASR)" on page 22 for instructions. (6501665)
- After replacing the power supply to a controller unit after a power supply failure, the Web Administrator might still show the file volumes as missing. (6498818)
- After creating a port aggregation (PA) bond, the Web Administrator might experience connection problems. (6400350)

- Adding NFS exports from the System Manager panel of the Web Administrator GUI fails. When the task is completed, viewing the exports from UNIX Configuration → Configure NFS → Configure Exports shows that the export has not been added. The export has actually been created, but it does not appear in the GUI. (6438697)
- On rare occasions after a LUN is successfully created using IBRM, the NAS OS can't get the LUN initialization status from the RAID controller. This causes the new LUN to not show up in the GUI RAID management screen. (6435497)
- Scheduled checkpoints might not be taken at their appointed time. A delay of up to 1.5 hours can occur. (6445966)
- If the TCP/IP host address and the TCP/IP gateway address are mistakenly typed with the same address, it is not possible to fix the error using the Web Administrator or the administrator console. You will continue to get duplicate IP address errors. (6441168)
- When configuring multiple NIC ports using the administrator console, entering the same IP address for more than one port does not result in an error. (6436496)
- The online help does not work from the Web Administrator on Solaris clients. (6428038)
- High Availability → Set LUN Path → Auto Assign LUN Paths will not work on new LUNs. (6397065)
- On new systems, or when you add a new controller or expansion unit, some LUNs might be offline. (6337658)
- There is no current method provided by the Web Administrator to bring volumes shown as offline in the screen RAID → Manage RAID online. (6331263)
- Firmware upgrade can take several hours for an appliance with an array with a large number of drives. (6519937)
- When deleting a HA/PA bond on a clustered system, the IP address of the bond might be assigned to a different unused port on the partner head. This could cause a link failure on the partner head and trigger a head failover. (6449658)
- If both Fibre Channel (FC) cables are pulled on one head, and then a recovery option is initiated from the other head, the system could go to the NORMAL state instead of the QUIET/ALONE state. The LUNs on the pulled Fibre Channels are also not available. (6436683)
- In a cluster configuration, before doing a recovery, check the partner head using the LCD to see if the head is in QUIET mode. Then do the recovery of the ALONE head from the Web Administrator or administrator console. (6229943)
- The ALONE head could remain in the transition state while the QUIET head is in the QUIET state. (6240366)
- Using the LCD or the reboot command to reboot one head of a cluster will also cause the other head to reboot. (6389192)

- After a mirror breaks, promoting a volume following a rename twice, the promoting operation works as if you were adding the mirror and not promoting it. (6433113)
- The Antivirus Configuration list accepts duplicate names if they have case (upper or lower) differences. (6436698)
- If a system is configured to use two scan engines, and one of them is stopped, the other scan engine also stops. An "access denied" message is displayed. (6433675)
- When enabling anti-virus protection for the first time, existing client connections to Common Internet File System (CIFS) mapped shares will be exempt from scanning and are not protected. (6417994)
- Under heavy I/O load with the Solaris iSCSI initiator, you might experience time-outs and/or receive protocol error messages. (6439416 / 6428783)
- When the Symantec Anti-Virus Scan Engine quarantines a file, the scan engine provides log information pertaining to its inspection of the file, but the file is over-written with this log information and thus the original file data is lost. (6418443)
- Installing new NICs will cause existing PA bonds to change roles which cannot then be deleted. (6407988)
- An attempt to promote a volume created with multiple segments in a mirror after the mirror is broken fails. (6387400 / 6437373)

Known Issues

The issues described in these sections are not resolved. If a solution is available, it is included. Change Request numbers are in parentheses.

- Importing a NetBackup image fails due to a difference in the way Sun Microsystem and Symantec have implemented NDMP.(6612128)
- If a change from workgroup mode to domain mode is done using an invalid password or insufficient permissions, the join operations fail although the security mode indicates the NT Domain. (6503245)

  Workaround: Enter the correct information and when prompted to reboot, reboot the system manually.
- A failed or offline drive is not logged in the syslog nor is a SNMP trap created on a 5210. No SNMP trap is created on 5220/5320 systems. (6512312)
- Poor RX/TX optical signal strength might result in degraded performance. (6207069)

  Workaround: If there are no other critical hardware errors and you see significant performance degradation, this degradation could be related to Fibre Channel link errors. Contact Sun Service for assistance. See "Service Contact Information" on page 5.

Web Administrator Issues

- When using the Web Administrator to delete multiple IP addresses at the same time for a port aggregation bond, the result can be the error message: "Configure NIC failed - Invalid IP Aliases"(6482862)

  Workaround: Either use the Web Administrator to remove the IP addresses in LIFO order (last in, first out) or use the CLI to remove the IP addresses.
- The administrator console and the Web Administrator are not consistent in how they accept space characters in the administrator password. (6502582)

  Workaround: Do not use spaces in the administrator password.
- The Web Administrator fails to release a lock intermittently, causing a pop-up window to be displayed with the message, "Server Locked." (6410459/6506346)

  Workaround: To release the lock, log out of the Web Administrator and log in. As an alternative, use the following command:

  ```
  datalock reset 0
  ```
- During LUN initialization, the View LUN Information panel might not show the proper LUN status.(6378027)

Workaround: Refresh the panel, or wait until LUN initialization is complete.

- Some volumes might remain unmounted if the `disk detach` command fails due to the existence of compliant volumes.

  Workaround: Manually mount all unmounted volumes.

- When you delete a volume that is bounded by a volume on either side with no free space is deleted, another volume of the same size cannot be created from the Web Administrator GUI. (6445486)

  Workaround: This is due to a rounding error. Create the volume by using the administrator console or CLI.

- Volumes with one or more attached segments might still appear in the Web Administrator GUI after being deleted. (6439670)

  Workaround: Log out of the Web Administrator, restart it, and log in again.

- The Add Quota window overwrites any existing quota settings without providing a warning. (6438298)

  Workaround: Verify the new settings before submitting the update.

- Creating two LUNs with volumes in secession creates both LUNs and volumes, but doesn't populate the Create File Volume screen and the View File Volume screen with the volume data from the second LUN. However, the Edit Volume Properties, Delete File Volumes, and Attach Segments screens do contain the data from both volumes. (6425260)

  Workaround: Perform a Scan for New Disks to populate the screens with the complete data.

- In a CIFS shared directory, files that are copied, deleted, or renamed are not updated.(6432492)

  Workaround: Use the F5 key to refresh the view on the Windows client.

- In-band RAID management (IBRM) does not prevent the deletion of a LUN in a Volume Group while that Volume Group is being rebuilt. (6443672)

  Workaround: Do not delete LUNs in a Volume Group while that volume group is being rebuilt.

- Moving files using drag and drop can cause the Microsoft Windows Explorer to hang for a few minutes if the directory has a Korean name from a Windows XP client.(6441365)

  Workaround: Wait a few minutes for the move to complete.

- NFS exports containing extended characters (UTF-8) cannot be mounted or viewed from EUC-KR clients. (6443034)

  Workaround: NFS clients using EUC-KR character sets can export only at the volume level. Volume names are restricted to ASCII.

- The CPU utilization reaches 100% when trying to run the `raidctl get` command using an rsh connection. (6376034)

  Workaround: Run the `raidctl get` command on the local system. Send the command's output file using `ftp`, email, or some other method.

- The In-Band RAID Management (IBRM) screen might display phantom tray instances with ID 0. (6396234 / 6398799)

  Workaround: These instances can be ignored safely. To update the display, perform a recovery process.

- When configuring a bond by selecting Networking Configuration → Configure Network Adapters, you can add the IP address only to bottom of the list, even if there is a blank field at the top of the list. (6401617)

  Workaround: To control the order of the list, you must delete all the IP addresses and add them in the order you want. As an alternative, use the CLI to configure the bond.

- SCSI errors might occur during writing to direct-attached SCSI LTO3 tape drives. (6347059)

  Workaround: Use the on-board Fibre Channel / SCSI bridge on the robot to connect to a Fibre Channel port on the NAS appliance or gateway system.

- When LUN creation requires several minutes to complete, the Web Administrator might provide ambiguous information. (6273163 / 6273171 / 6276198)

  Workaround: Close the Web Administrator and browser. Open a new browser and restart the Web Administrator.

- Upgrading firmware using In-Band RAID Management (IBRM) might cause all LUNs on the Sun StorEdge 6130 array to fail over to a single RAID controller. (6283300)

  Workaround: Place the LUNS on the primary path.

- The Notification Email URL field shows the hostname but when you click on it, you do not connect to the Web Administrator. (6217684)

  Workaround: If the name server does not resolve the hostname, use the IP address to connect. To prevent this condition, verify that the host name entered for notification is registered in a name server (for example, DNS or Network Information System (NIS)).

- After you delete a bond, the IP address for a High Availability and Port aggregation bond is not restored properly. (6212483)

  Workaround: Select a different IP address for the bond.

- When you select Configure NFS → Setup Hosts → Add User, the changed information does not display and the system appears to stop working. (5054655)

  Workaround: If the NIS or NIS+ database has many mappings, you must wait for the system to finish processing. Do not reboot your system.

Copy Issues (rsync)

- When using both rsync and NDMP, if you issue one command while the other operation is still running, both operations succeed but performance is poor. (6557706)

  Workaround: Avoid performing an rsync operation on a volume during a backup operation of that volume. Wait until the first operation is complete before issuing the second command.

- In a cluster configuration, if an ssh client is connected to a head that fails over to the second head, the rsync operation is interrupted because the ssh client does not recognize the second head.

  Workaround: Establish a new ssh connection to the second head, now in the ALONE state. (6556518)

- Because rsync uses ssh, a problem with ssh is observed when you use rsync. If the NAS appliance does not require a password, an rsync operation displays a prompt for one. (6557009)

  Workaround: Enter any text at the prompt and the rsync operation continues.

Backup Issues (NDMP)

- For information about changes needed when upgrading to Version 4 of NDMP, see "Upgrading to NDMP V4" on page 28.
- In a cluster system, do not attach both NAS heads to the same tape drive because if one head fails during a backup, data on the media can be lost. (6527152)
- NDMP V2 is not supported, but an attempt to backup a system that uses the V2 protocol is not prevented and will cause an error. (6528317)
- When you replicate a volume, the resulting volume is identified with the type "nbd." This type of volume does not have a checkpoint and therefore attempts to back up the data fail. (6563888)

  Workaround: Create a checkpoint for the file system manually, using the following procedure:

1. On the replicated volume, create a checkpoint, for example, test.
2. On the mirror system, verify the checkpoint using the ls command:

   ```
   ls /volume_name.chkpnt/test
   ```

3. From the DMA, edit the default path to specify the complete checkpoint path, that is, from the volume name to /*volume_name*.chkpnt/test
4. Back up the replicated volume.

Antivirus-Specific Issue

The following antivirus-specific issue is not resolved at this time:

- The Trend Micro scan engine reports a file larger than 2GB incorrectly as corrupted. (6505262)

  Workaround: In the Antivirus Configuration panel, set the Max Scan Size to a value less than or equal to 2GB.

Array Firmware-Specific Issues

- The communication between the LUN path and the Controller fails. (6504220)

  Workaround - Reset the controller and the NAS 5320 C appliance.

- The over temperature alarm on a 6140 array does not turn on the tray fault amber LED. (6490889)

  Workaround - Check the NAS system log file for messages that indicate over temperature.

- MPP is able to reconcile only two out of the four LUNs when four initiators are assigned to two hosts on the same array. (6503637)

  Workaround

  - Assign all four initiators to one host.
  - Assign different LUN numbers to the volumes from each host.
  - Assign both hosts to a host group and then map the volumes to that host group.

- You might receive an incorrect email message stating that a critical error has been logged for a full file system. (6517078)

  Workaround - Verify that the file system is not full.

- Removing multiple hot spare drives from a tray and reinserting them can result in a drive having its LUN remain in a degraded state. (6502481)

  Workaround - Remove hot spare drives and replace failed drives one at a time.

Cluster-Specific Issues

- When you assign a LUN to a server in a gateway cluster configuration, you must manually scan the disk on both servers to pick up the new LUN. Otherwise, the new LUN on the current server is not recognized by the partner server and the mismatch can cause the partner server to reboot. (6577612)

Use the following procedure when adding a LUN in a gateway cluster:

1. On the current server, use the Web Administrator to navigate to Volume Operations > Create File Volumes and then click Scan for New Disks.

2. On the current server, navigate to High Availablity > Recover and assign the LUN ownership to the desired server and click Apply.

3. On the partner server, navigate to Volume Operations > Create File Volumes and then click Scan for New Disks.

4. On the current server, navigate to High Availablity > Recover and then click Restore to move the LUN to the server that owns the LUN.

- The Web Administrator supports multiple logins at a time. However, multiple logins from the Web Administrator and administrator console or CLI is not supported. In a cluster configuration, you must log in to each server separately to manage that server.

- Cluster recovery fails when a LUN is offline and a server is in the ALONE state, causing both servers to have incorrect LUN information.(6480807)

  Workaround: Reboot the ALONE server a second time and then repeat the recovery.

- After reassigning a primary slave NIC on Head 1, an HA bond goes into failover mode on Head 2, resulting in an inability to connect to Head 1 using either the Web Administrator or the administrator console. (6485209)

  Workaround: Log in to the system console and recover the bond on Head 2. Reassign the primary slave on Head 1 and recover the bond on Head 2.

- Using the Web Administrator to change the Down and Restore Timeout value will update the partner server but not the current server. (6497601)

  Workaround: Use the administrator console to modify the value.

- When a server is in the ALONE state, it is possible to create an HA/PA bond. It is not possible to delete a bond. (6508824)

  Workaround: Do not modify bonds while the server is in the ALONE state. Creating or deleting bonds in the ALONE state causes inconsistencies.

- If both Fibre Channel (FC) cables are pulled on Server 2 and then restored, a volume might not be mounted. (6435436)

  Workaround: Mount the volume manually.

- If the configuration wizard was used to set up the cluster and failover was enabled on only one server, you cannot enable failover on the partner server. (6387567)

  Workaround: Use the Web Administrator to log into the partner server and enable failover.

- If the QUIET server experienced system problems during recovery, some of its volumes might fail to mount on the ALONE server. (6214772)

  Workaround: Use the following command to mount a volume:

```
hostname> mount -f /volume-name
```

- A server can modify file permissions only on file systems owned by that server and not on those owned by the partner server. (6262339/6222886)

Sun StorageTek File Replicator Issues

The following replicator-specific issues are not resolved at this time. Change Request numbers are in parentheses.

- The Promote With Rename function does not rename both volumes and shares. Although the volume is renamed, the share on the mirror remains pointing to a volume with the original name.(6490007)

  Workaround: Remove the share and create a new share that points to the volume with the changed name.

- Removing a Sun StorageTek File Replicator license and reinstalling it might cause problems in reestablishing a new sync. (6507058)

  Workaround: After reinstalling the license, reboot the system.

- When configuring a network card, you are not prevented from entering a zero (“0”) in the first segment of the IP address, resulting in an invalid address. (6424098)

  Workaround: Do not enter a zero (“0”) in the first segment. The address must be valid.

- After a refresh of the display, the View Mirror Statistics panel might not display mirrored volumes. (6438307)

  Workaround: In the left-side Navigator Tree of the Web Administrator, select another node. Then select the node displayed previously. If the mirrored volumes are still not displayed, log out of Web Administrator and close the browser. Open a new browser window, restart the Web Administrator, and log in again.

- More than 52 volumes cannot be displayed in the administrator console’s Add Mirror menu so you cannot add more mirrored volumes.(6441717)

  Workaround: Use the Web Administrator to create more mirrors.

- When you use file replication in a cluster, a change role on the master cluster followed by a cluster failover results in a mirror loss because the change role does not conclude its operation. (6428902)

Workaround: Use the CLI to unset the `mirror.changerole` parameter and then establish mirroring.

- After renaming a volume, operations such as change role or break/promote from the target fails. (6437381)

  Workaround: Unmount the volume and then remount it.

- An attempt to promote a volume created with multiple segments in a mirror after the mirror is broken fails. (6437381)

  Workaround: Avoid this problem by unmounting and remounting the volume after renaming or attaching segments. The volume can be replicated after it has been remounted. Alternatively, the head can be rebooted instead of unmounting/remounting the volume. The target system (mirror) is not affected and does not need to be rebooted.

- If there is a system failure such as a power failure within 10 seconds of the start of a change role process, both systems might be set as the TARGET and there will be no MASTER, causing loss of the mirror. (6198655)

  Workaround: Contact Sun Technical Support for help in establishing your mirror.

- If you do a Change Role operation while there is heavy I/O activity on the master volume, the master might time out and you might lose CIFS access to the volume. (6248243)

  Workaround: Unmount the volume and then remount it.

- The RESYNC option is not available in the Web Administrator. (6198789)

  Workaround: Use the administrator console.

iSCSI-Specific Issues

The following iSCSI-specific issues are not resolved at this time. The numbers in the parentheses indicate the Change Request.

- The CLI and administrator console does not prevent you from creating an iSCSI LUN on system volumes: cvol, dvol, tmp, proc, checkpoint, or readonly volumes. (6515138)

  Workaround: Do not create iSCSI LUNs on system volumes.

- An iSCSI login might result in a rejection due to too many connections. (6444187)

  Workaround: An iSCSI session supports four simultaneous connections to the NAS appliance or gateway system. Wait approximately a minute for old sessions to time out and log in again.

- After adding access list members on Head1, the initiator IQN Name might be incorrect for Head2. (6426391)

Workaround: Make another change to the access list and save to force the list to update Head 2.

- Execution of an I/O operation with DataDigest Enabled results in DataDigest errors from Solaris clients. This is due to the zero copy implementation of the Solaris iSCSI initiator. (6446747)

  Workaround: Do not use Data Digest with Solaris clients. If Data Digest is needed, use an iSCSI HBA implementation.

Documentation Issues

The following issues have been identified in the documentation:

- Problem: In the Getting Started Guide (819-4283-11), on page 67, is the following text: “To connect a controller unit and two expansion units, four 2-meter...”

  Correction: This sentence should refer to a controller enclosure, not a controller unit.

- Problem: In the Getting Started Guide (819-4283-11), on page 131, the sentence starting “The two scripts...” is duplicated.

  Correction: The sentence that has the linked URL is correct.

- Problem: In the Getting Started Guide (819-4283-11), on page 131, a step in the procedure is not formatted properly.

  Correction:

  - Step 5 should have this example:

    ```
    # Smcli IP_address_controller_B -f CtrlBModRegion12
    ```

  - Step 6 should be "Reset controller A"
  - The command example for Step 6 is:

    ```
    # Smcli IP_address_controller_A -c...
    ```

    similar to the command example in Step 7.

Addenda to the Documentation

This section includes information that is additional to or overrides information in the documentation. It contains the following topics:

- "About the McAfee Secure Internet Gateway" on page 19
- "About the rsync Protocol" on page 20
- "About Online System Registration and Auto Service Request (ASR)" on page 22
- "Creating a Core Dump File" on page 24
- "Collecting Information for Configuration" on page 26
- "Exempting a Host Group from Virus Scans" on page 28
- "Upgrading to NDMP V4" on page 28
- "Restrictions on Sun StorageTek File Replicator" on page 28
- "Using a Sun StorageTek 5320 NAS Expansion Unit With a Sun StorEdge 5300 RAID EU Controller Enclosure" on page 30
- "Using a Sun StorageTek 5320 RAID Controller Unit With a Sun StorEdge 5300 RAID CU Controller Enclosure" on page 30

About the McAfee Secure Internet Gateway

You can use a McAfee Secure Internet Gateway 3000, 3100, 3200, and 3300 appliance or the McAfee Secure Web Gateway 3400 appliance that runs a minimum of SCM Version 4.21 Patch 5, to scan files stored on the Sun StorageTek NAS device. The McAfee appliance works in the same way as the other supported scan engine software products, as described in the online Help and in Chapter 4 of the *Sun StorageTek NAS OS Administration Guide* (819-4284-*nn*).

To perform the antivirus scans, configure the McAfee appliance with the following attributes:

- Verify that the McAfee appliance is running the minimum supported software, Version 4.21 Patch 5. If not, you can obtain it from the McAfee SCM Support page.
- Change the Response Modification Service Settings service path to `/avscan` from its default path of `/RESPMOD`.
- For efficient performance, change the value for the ICAP Policy Protocol's Transfer-Complete attribute to the * character, if it is not already set.

About the rsync Protocol

The rsync protocol transfers new files and changes to existing files between a Sun StorageTek 5000 NAS system and a remote system. Use rsync for purposes that require more efficiency than the ftp protocol and more control than the rcp protocol, but do not require a real-time replication solution such as the Sun StorageTek File Replicator option. It is most efficient when the file exists on both systems and only changes are transferred.

Restrictions on rsync

The implementation of the rsync protocol in this release has the following limitations (6544680):

- The connection between the NAS system and the other location must use ssh. A direct connection is not secure and cannot be supported.
- The protocol is supported in server mode only. This means that the remote system initiates the transfer, either by sending file system objects to the NAS head or by copying file system objects from the NAS head.
- The rsync protocol's daemon mode is not supported.
- The ACLs of file system objects or any extended attributes are not saved.
- The only user supported for logging in and performing operations is the admin user.

Configuring rsync

The rsync feature is disabled by default. To use the feature at any time, issue the following command before using the rsync command:

```
load rsync
```

To enable the rsync feature, edit the inetload.ncf file to load rsync each time the NAS system reboots, using the following procedure:

1. Edit the inetload.ncf file, located in the /dvol/etc directory.
2. At the end of the file, add a comment and the command:

```
# The rsync module provides remote copy of incremental file changes.
# YYYY:MM:DD
rsync
```

3. Save and close the file.
4. Issue the following commands to use the new version of the inetload.ncf file:

```
> unload inetload
> load inetload
```

The rsync protocol is now enabled in the current session and will be enabled after any system reboot.

Using rsync

This release supports the rsync protocol in server mode. This means that from the system where you are logged in, you can copy file system objects from your system to the NAS head or you can copy file system objects from the NAS head to your system.

The general procedure for using the rsync protocol is to log into a network system, issue the rsync command, specifying the files to be copied. The rsync command uses the system's ssh client to transfer the files.

1. Log in to a network system. This example uses a Windows system.
2. Click Start > Run from your Windows desktop.
3. In the Run window, type cmd and click OK.
4. Enter the rsync command, using the following syntax:

```
>rsync [OPTIONS] source_location destination_location
```

where both source_location and destination_location are the current directory or one specified in the format: *[USER@]hostname:directory_name.* The hostname is the IP address or DNS name, the single colon specifies that the transfer uses the ssh client, and the directory_name is the path.

For example, to copy changes to files in the current directory on the system you are logged into (local) to the NAS appliance in your network (remote_nas) in its Monday directory, use the following command:

```
rsync [OPTIONS] * remote_nas:Monday
```

To retrieve files that might have changed from the NAS appliance and put them in the local Wednesday directory, use the following command:

```
rsync [OPTIONS] remote_nas:Monday/* Wednesday/*
```

To see all the options and a description of the command as it is implemented in your network, use one of the following command on a network system:

```
>man rsync
>rsync --help
```

The rysnc process copies the following:

- If the file does not exist at the destination, it copies the file.

- If the file exists at the destination, it copies the changes to the file.

About Online System Registration and Auto Service Request (ASR)

The online Help and *Sun StorageTek NAS OS Administration Guide* describe the Online System Registration feature but do not emphasize that, in addition to registering the system, this feature monitors the system and can generate automatic service requests (ASR). This feature notifies the Sun Technical Support Center when events that generate a critical alarm occur.

ASR is available to all customers with current StorageTek Warranty or StorageTek Spectrum Contracts. The service is available from activation until the end of warranty or contract period. The service levels are based on the contract level and response times of the connected devices. The ASR service uses SSL security and your Sun online account credentials to authenticate transactions but does not monitor stored data. The feature collects only the following information:

- Activation event: Static data collected for purpose of registration and entitlement.
- Heartbeat event: Dynamic data collected daily to establish whether a device is capable of connecting.
- Alarm event: Critical events received through the secure transport, triggering Service Requests.
- Alert event: Additional events collected to provide context for existing or imminent cases. Not all events sent to Sun Microsystems open a Service Request. Only critical events that require Sun Service to fix are opened automatically and sent to your local Sun Technical Support Center.

Details and security documentation are available at http://www.sun.com/service/remoteconnectstorage.

Requirements for Online System Registration and ASRs

Each NAS system must be enabled individually and meet the following requirements:

- Sun StorageTek NASOS firmware, version 4.21.M1 and higher.
- A Sun Online Account. This is the same account used for the Sun Download Center (SDLC). To obtain an account, go to: `http://javashoplm.sun.com/ECom/docs/Welcome.jsp`
- An outbound-only HTTP connection through port 443 using HTTPS (HTP with TLS) to communicate with Sun Services. The connection can be direct or by proxy.
- Ability to resolve Domain Name Service lookups.

Enabling Online Registration and ASRs

You configure the registration using the Web Administrator's Online Registration Panel. To register the system, log into the Web Administrator and do the following:

1. From the navigation panel, choose System Operations > Online System Registration.
2. Read Sun's privacy policy and disclaimer. To continue, click the Agree button.
3. If you do not have a Sun Account, click on the here link at the bottom of the dialog. This opens the Sun Online Account Registration portal. Click Register to begin to create the account.
4. If you have a Sun Account, type its ID in the Sun Account ID and enter its password.
5. Click Next to go to the Proxy Server tab.
6. If your site will use a proxy server, enter the name of the proxy server you want Sun Services to use and its port number. If the proxy server uses authentication, enter its user name and its password.

The information for registration is complete. To enable the Auto Service Request feature:

7. Click Next to go to the Options tab.
8. Select both options: Send Heartbeat Data and Send Fault Events. The heartbeat data is a daily check without regard to the type of event. The fault events are sent when a failure is occurring.
9. Read the Purpose statement and click OK to submit the request.

Your site's contact email account receives a confirmation message that the system has been activated. The Online System Registration dialog identifies the system as Registered.

If you prefer to stop sending heartbeat or fault events to Sun Services, use the same procedure to display the Options tab and clear the checkboxes. The system remains registered but the information is not sent.

Creating a Core Dump File

A serviceability enhancement in version 4.21 was a diagnostic email message that support engineers can use to diagnose and solve problems. For some specific problems, the support engineer might need to perform a core dump analysis, which requires a core file. A core file contains a snapshot of the contents of physical memory when a system crash occurs.

The following procedure configures the NAS server to capture a core dump and save it as a file in a directory on the backend storage. When you complete the procedure, the next system failure or panic saves the core dump data to a raw disk partition and, after the system reboots, then saves the data to a file, leaving the raw disk partition available for any future core dump procedures. For more detail on core dump files and advanced configuration, see document 89129 in the SunSolve Knowledgebase, located on the SunSolve site, `http://sunsolve.sun.com`.

Note – Do not perform this procedure unless a support engineer requests a core file.

---

1. To make a raw disk partition of sufficient size to capture the size of physical memory, log into the administrator console and make the following selections:

   a. From the Configuration menu, choose Disks & Volumes.

   b. Identify a drive with at least 6 GB of available space and that does not already have a raw partition.

   c. Type the letter of the drive to select it.

   d. Choose 1, Edit.

   e. Use the arrow keys to scroll to the desired free space.

   f. Select 1, Create.

   g. Select 3, Raw.

   h. For size, enter 6000.

   i. Select 7, Proceed with create.

2. Press the Esc key to display the command line.

3. Identify a directory location to store the core files or create a new one. Do not use `/cvol` or `/dvol` flash storage.

4. Enter the following commands:

```
set kern.dumpdir /volume/path
```

```
savevars
```

where */volume/path* is the path to an existing directory to store the core files.

5. If you have a cluster configuration, repeat this procedure for each NAS head in the cluster.

6. If it is possible to create the conditions under which the system panics or an NMI is generated, perform those actions. The system then reboots.

After the system reboots, the core file is saved in the directory you specified, with the filename, `vmcore.x.gz`, incrementing *x* for each new core file.

Configuring Quotas With Limits

The following information was not included in the description of the Configure User and Group Quotas Panel: (5058072)

Hard and Soft Limits

A hard limit is the absolute maximum amount of space available to the user or group. When a user's or group's storage reaches a soft limit, which is equal to or lower than the hard limit, a grace period of seven days starts in which files can be removed. After the grace period, the user or group cannot write to the volume until the amount of space used is below the soft limit.

The hard limit must be equal to or higher than the soft limit. For disk space, it can be no more than approximately 2 terabytes. For the number of files, the hard limit can be no more than 4 billion files.

The root user and root group do not have hard or soft limits for space or files and cannot have quotas defined.

Collecting Information for Configuration

You configure the Sun StorageTek NAS OS software using the Web Administrator's Configuration wizard. The following worksheet lists information you can gather before you start the wizard, depending on the type of environment you select: Windows Only, Unix Only or Both. (6250174)

TABLE 1 Sun StorageTek NAS 5000 Family Configuration Worksheet

For All environments	
For Server Name, a string to identify this NAS appliance. Begin with a uppercase or lower case character or number 0-9, can include hyphen, underscore, or period character. Limit is 30 characters.	
For Contact, the name of your company, department, or unit. This string will be included in diagnostic messages.	
Network adapters If your network does not use a Dynamic Host Configuration Protocol (DHCP) server, you must specify a static IP address for each network port: >Internet Protocol (IP) address >netmask >network interface card (NIC) port role >alias IP address (optional)	
Default gateway IP address	
For Windows or Both environment	
For Domains and Workgroups Active Directory Service (ADS): Name of this NAS appliance's domain: Username and password of a domain user or, if ADS, the Windows 2000 user who is domain administrator. For ADS Container, the ADS path location of the Windows 2000 administrative user in LDAP distinguished name (DN) notation (common name and organizational unit). Do not include the domain name in the path. For Site, the site name. Specify if the ADS domain controller is in a different subnet than this NAS appliance. For Workgroup Name, the name of an existing group	
For configuring the NAS appliance as a Windows Internet Naming Service (WINS) client: IP address of the server for NetBIOS name resolution. IP address of a server to be contacted if the first WINS server does not respond. Name of this NAS appliance's domain	
For DNS Server, either the IP address of a new one or the name of an existing one Name of the domain that contains this NAS appliance	
For UNIX or Both environment	

TABLE 1 Sun StorageTek NAS 5000 Family Configuration Worksheet

For DNS Server, either the IP address of a new one or the name of an existing one **Name of the domain that contains this NAS appliance**	
For Network Information Service (NIS) Name of the domain the NAS appliance uses for NIS services **Either the IP address of a new NIS server or the name of an existing one. If you do not know the IP address, you can let the server be acquired.** **For NIS+ (name service with added security), configure NIS+ after you complete the wizard.**	
For LDAP Server: Name of the domain that contains the LDAP server **Password for the domain server.** **IP address of the LDAP server.** **If you use a proxy domain, the name of the proxy.**	
Identify the lookup order of the name services to use for each type: **>user** **>group** **>netgroups** **>hosts.**	
For All environment	
For Email Notification, either the IP address of your SMTP server or the DNS name of your SMTP server **Up to 4 email addresses to receive notification messages**	
For a remote log: Either the DNS host name or the IP address of the system where system log will reside. **For a local log: Full path and filename of the log file.** **Specify the number and size of archive files**	
Specify time, date, and working language	
For registering the system for online Sun Service, your Sun Account ID and password. **The ID for an outbound-only HTTP connection through port 443 using HTTPS or if your network uses a proxy server, the name of the proxy server and its port number. This server might require a username and password also.**	

Using a Sun StorageTek Flexline 380

To use the Sun StorageTek NAS 5320 Gateway Appliance with a StorageTek Flexline™ FLX380 enterprise storage system that has FLA/FLC expansion trays, you must run a script to create a host entry in the NVSRAM for the NAS LUNs. Patch 124128-01 contains the scripts and instructions, available from http://sunsolve.sun.com

Exempting a Host Group from Virus Scans

Using the `/dvol/etc/approve` file to exempt a host group as documented does not exempt the share from scanning. The correct syntax for exempting a host group in the approve file includes an `@` symbol, as in the following:

`vscan` *sharename* `@`*hostgroup* `access=noscan`

An alternative is to use the Configure Share function. (6540932)

Restrictions on Sun StorageTek File Replicator

- It is not possible to mirror volumes of size exactly equal to 1024 MB or 1 GB as stated in the documentation. The minimum "raw" size of a mirrored volume is 1046 MB. (6440799)
- Volumes that have greater than 90% utilization cannot be mirrored. The documentation only states that the minimum buffer space that can be defined is 100 MB. In addition to the 100 MB minimum requirement, the mirror buffer cannot be larger than 50% of the available free space. (6440868)

Upgrading to NDMP V4

With this release, the default version of NDMP is V4. The NDMP client is a data management application (DMA) and it must be changed to continue to work with systems running this release:

- Change the DMA to use NDMP V4 so that it can be a client of systems that use either V4 or V3. By setting the DMA to use NDMP V4, the DMA uses the V4 protocol as a client to NAS OS 4.21 systems and can use the V3 protocol as a client to other systems that support only NDMP V3. If the DMA remains set to V3, it can be a client to a system running NAS OS 4.21 but will use the V3 protocol.
- Change the name of the administrator account. The administrator account is now "admin" instead of the name "administrator" used in version 4.20 and previous versions.
- Change the drive paths. The format of the drive paths and the paths themselves have changed.(6517142) To obtain the proper drive paths, run the following command from the command line:

  ```
  ndmp devices
  ```

  For example, the format of the drive path for robot and jukeboxes has changed from `isp1m001` to the following:

  ```
  /dev/scsi/changer/0
  ```

  where `0` is the target ID

The format for the drive path for a tape drive has changed from `isp1t001` to the following:

```
/dev/rmt/0
```

where `0` is the target ID

- Change the log path. After an upgrade, the log path is reset to the default location, `/dvol/etc/backup`. Specify the full path to a valid volume used to store intermediate backup data and the permanent log of backup history. The file name remains ndmp.log.
- Any NDMP bitmap files created during a backup operation are deleted automatically. Occasionally, for example, when multiple file volumes are backed up in a single backup job, some NDMP bitmap files, named `ndmp.n,` might remain. These can be deleted. (6184861)

Using a Sun StorageTek 5320 NAS Expansion Unit With a Sun StorEdge 5300 RAID EU Controller Enclosure

This release of the NAS OS software enables you to configure a new expansion unit as back-end storage for a Sun StorEdge 5310 system that has the Sun StorEdge 5300 RAID EU Controller Enclosure. After a firmware upgrade, the controller enclosure can recognize and manage the new expansion unit. TABLE 2 shows which configurations are supported and where the procedures are documented.

TABLE 2 Supported Combinations of Controllers and Expansion Units for Sun StorageTek 53xx NAS Systems

	Controller	
Expansion	**Sun StorEdge 5300 RAID EU Controller Enclosure**	**Sun StorageTek 5320 RAID Controller Unit**
Sun StorEdge 5300 EU Expansion Enclosure	Supported for Sun StorEdge 5310 and Sun StorageTek 5320 NAS systems and documented in: • *Sun StorEdge 5310 NAS Appliance and Gateway System Getting Started Guide* • *Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide* (819-4283-nn)	Not supported.
Sun StorageTek 5320 Expansion Unit	Supported in Sun StorEdge 5310 and Sun StorageTek 5320 NAS systems with 4.20.M3 software (minimum) and documented in the release notes for that release and also *Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide* (819-4283-11)	Supported for Sun StorageTek 5320 and documented in *Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide* (819-4283-11)

Using a Sun StorageTek 5320 RAID Controller Unit With a Sun StorEdge 5300 RAID CU Controller Enclosure

This release of the NAS OS software enables you to configure an existing Sun StorageTek 5320 NAS appliance with two types of controllers: a 5320 RAID controller unit and an 5300 RAID controller enclosure. After a firmware upgrade on the appliance, it can recognize both types of controllers and manage them. However, each controller stores data in separate back-end storage independently of the other controller. The advantage of this configuration is to improve I/O throughput but the disadvantage is the storage arrays are independent and do not provide failover protection for each other. This configuration and procedure does not apply to Sun StorageTek 5320 NAS Gateway systems or Sun StorEdge 5310 NAS systems.

▼ To Upgrade Array and Drive Firmware on 5300 and 5320 RAID Controllers

Use this procedure to upgrade the array and drive firmware to run a Sun StorageTek 5320 NAS appliance with both a StorEdge 5300 RAID controller and StorageTek 5320 RAID controller. The NAS server updates each controller with different files, one at a time, when it is powered on. In general, the plan for upgrading the controllers is the following:

- Download the new firmware for one controller to the NAS server.
- Power down the other controller.
- Power cycle the NAS server to upgrade the first controller.
- Verify the new firmware is in effect.
- Download the new firmware for the second controller to the NAS server.
- Power down the first controller to prevent its new firmware from being overwritten.
- Power cycle the NAS server to upgrade the second controller.
- Verify the new firmware is in effect.
- Power on the first controller.

This procedure upgrades the 5300 RAID controller first and then the 5320 RAID controller.

Note – Follow the power cycle instructions exactly because the server upgrades the controller during that process.

1. **Download the latest patch from `www.sunsolve.sun.com` and unzip the file.**
2. **Review the patch readme file to determine which firmware revision levels are associated with the patch.**
3. **From a Sun StorageTek 5320 NAS Appliance, enable** `ftp`**. Refer to the *Sun StorageTek NAS OS Administration Guide* for information about how to enable** `ftp` **using the Web Administrator or CLI.**
4. **Change to the directory where you downloaded the patch.**

▼ To Upgrade the Sun StorEdge 5300 RAID Controller

5. **Use** `ftp` **to connect to the Sun StorageTek 5320 NAS Appliance or, in a cluster configuration, server 1. Log in as the admin user.**

6. **Enter `bin` for binary mode.**

7. **At the** `ftp` **prompt, create the following directories on `/cvol` by entering these commands:**

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
mkdir /cvol/firmware/2882/drive
```

8. **Use the `put` command to copy each file to the appropriate directory:**

```
ftp> put filename /cvol/newdir/filename.ext
```

Firmware files are truncated after they are copied to their directories. TABLE 3 shows example directory and firmware file names.

TABLE 3 Directory and Firmware File Examples for 5300 RAID Controllers

Component	Directory	Example File Name
RAID controller	/cvol/firmware/2882/ctlr	SNAP_288X_06120910.dlp
RAID controller NVSRAM	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
Fibre Channel EU	/cvol/firmware/2882/jbod	esm9631.s3r
SATA EU	/cvol/firmware/2882/jbod	esm9722.dl
Drive Firmware	/cvol/firmware/2882/drive	D_HDS7250SASUN500g_0604

9. **Log out of the** `ftp` **session.**

10. **Power down the NAS server. In a cluster configuration, power down both server 1 and server 2.**

11. **Power down the StorageTek 5320 RAID controller and all attached trays. Do not power down the StorEdge 5300 RAID controller or its trays. The controller must be powered on to be upgraded.**

Note – Do not power down the RAID controller while the upgrade is in progress. Upgrade times can vary.

12. **Power up the NAS server or server 1.**

    When the NAS server is powered on, it downloads the new firmware to the StorEdge 5300 RAID controller and then removes the files.

Note – In cluster configurations, do not power on server 2 at this time. If server 1 comes up in QUIET mode, select the TAKE ALL LUNs command from the LCD.

---

13. **Use the administrator console to connect to the NAS server or server 1, and log in to a user account with admin privileges.**
14. **Verify that the new firmware has been loaded by entering this command:**

    ```
    raidctl get type=lsi target=profile ctlr=0
    ```

    Check the system log for failures and to make sure that downloading is complete.

▼ To Upgrade the StorageTek 5320 RAID Controller

15. **Change to the directory where you downloaded the patch.**
16. **Use `ftp` to connect to the NAS server or server 1, and log in as the admin user.**
17. **Enter `bin` for binary mode.**
18. **At the `ftp` prompt, create the following directories on `/cvol` by entering these commands:**

    ```
    mkdir /cvol/firmware
    mkdir /cvol/firmware/399x
    mkdir /cvol/firmware/399x/ctlr
    mkdir /cvol/firmware/399x/nvsram
    mkdir /cvol/firmware/399x/jbod
    mkdir /cvol/firmware/399x/drive
    ```

19. **Change to the same directory that you created for the previous firmware. Those files have been removed.**
20. **Use the `put` command to copy each file to the appropriate directory:**

```
ftp> put filename /cvol/newdir/filename.ext
```

Firmware files are truncated after they are copied to their directories. TABLE 4 shows firmware file names and directories.

TABLE 4 Directory and Firmware File Examples for 5320 RAID Controllers

RAID controller	`/cvol/firmware/399x/ctlr`	`SNAP_399x_06192510.dlp`
RAID controller NVSRAM	`/cvol/firmware/399x/nvsram`	`N399x-619843-502.dlp`
EU	`/cvol/firmware/399x/jbod`	`esm9884.esm`
Drive Firmware	`/cvol/firmware/399x/drive`	`D_HDS7250SASUN500G_0604`

21. **Log out of the `ftp` session.**

22. **Power down the NAS server or server 1.**

23. **Power down the StorEdge 5300 RAID controller and all attached trays.**

Note – Do not power down if the upgrade is in progress. Upgrade times can vary.

---

24. **Power up the 5320 RAID controller and all attached trays.**

    You powered the RAID controller down in Step 11 but it must be powered on so that the NAS server can upgrade its firmware.

25. **Wait until the LEDs on the StorageTek 5320 RAID controller and its trays display as solid.**

26. **Power on the NAS server or server 1.**

    When the NAS server is powered on, it downloads the new firmware to the StorageTek 5320 RAID controller and then removes the files.

Note – In cluster configurations, do not power on server 2 at this time. If server 1 comes up in QUIET mode, select the TAKE ALL LUNs command from the LCD.

---

27. **Use the administrator console to connect to the NAS server or server 1, and log in to a user account with admin privileges.**

28. **Verify that the new firmware has been loaded by entering this command:**

    ```
    raidctl get type=lsi target=profile ctlr=0
    ```

    Check the system log for failures and to make sure that downloading is complete.

29. **Power down the NAS server. In a cluster configuration, power down both server 1 and server 2.**

30. **Power up the StorEdge 5300 RAID controller and its trays.**

    At this point, both the StorEdge 5300 and StorageTek 5320 RAID controllers and their trays are powered on.

31. **Wait until the LEDs on the StorEdge 5300 RAID controller and its trays display as solid.**

32. **Power on the NAS server. In a cluster, power on both server 1 and server 2.**

Note – If you are running a cluster system and server 2 powers up in QUIET mode, run a recovery from server 1. If you ran the TAKE ALL LUNs command in Step 12 or Step 26, you might need to distribute LUNs also.

Release Documentation

The following documentation is posted on the documentation Web site at:

`http://www.sun.com/hwdocs/Network_Storage_Solutions/nas`

Title	Part Number
Sun StorageTek NAS OS Administration Guide	819-4284-*nn*
Sun StorageTek 5320 NAS Appliance Setup [poster]	819-4385-*nn*
Sun StorageTek 5320 NAS Gateway System Setup [poster]	819-4286-*nn*
Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide (Sun StorageTek 5320 back-end storage)	819-4283-*nn*
Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide (Sun StorEdge 5300 back-end storage)	819-6387-*nn*
Sun StorageTek 5320 NAS Appliance and Gateway System Storage Regulatory and Safety Compliance Manual	819-7315-*nn*
Sun StorageTek 5320 NAS Array Regulatory and Safety Compliance Manual	819-6048-*nn*
Sun StorageTek 5220 NAS Appliance Setup [poster]	819-7166-*nn*
Sun StorageTek 5220 NAS Appliance Getting Started Guide	819-7167-*nn*
Sun StorageTek 5220 NAS Appliance Regulatory and Safety Compliance Manual	819-7366-*nn*
Sun StorageTek 5220 NAS Array Regulatory and Safety Compliance Manual	819-7367-*nn*
Setting Up the Sun StorEdge 5310 NAS Appliance [poster]	819-1168-*nn*
Sun StorEdge 5310 NAS Gateway System Poster	819-3240-*nn*
Sun StorEdge 5310 NAS Appliance and Gateway System Getting Started Guide	819-3237-*nn*
Sun StorEdge 5310 NAS Appliance and Gateway System Administration Guide	819-3238-*nn*
Sun StorEdge 5310 NAS Appliance Safety and Compliance Guide	819-0881-*nn*
Sun StorEdge 5210 NAS Appliance Administration Guide	819-5376-*nn*
Sun StorEdge 5210 NAS Hardware Installation, Configuration, and User Guide	817-6660-*nn*
Sun StorEdge 5210 Expansion Unit Safety, Regulatory, and Compliance Manual	817-7515-*nn*
Sun StorEdge 5300 RAID Expansion Unit and Sun StorEdge 5300 Expansion Unit Safety and Compliance Guide	819-0882-*nn*