Sun StorageTek™ 5320 NAS Appliance and Gateway Administration Guide

NAS Software Version 4.12

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6388-10
May 2006, Revision A

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

Please
Recycle

Contents

Figures

Tables

Preface

The *Sun StorageTek 5320 NAS Appliance and Gateway System Administration Guide* is a combined administrator's and user's guide for the Sun StorageTek™ 5320 NAS Appliance, the Sun StorageTek™ 5320 NAS Cluster Appliance, and the Sun StorageTek™ 5320 NAS Gateway System. This guide describes how to use the Web Administrator software to set up and monitor the system. It also includes instructions on using the command-line interface (CLI) and additional details about any system hardware that is not documented in the *Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*.

Before You Read This Book

Before reading this guide, you must have installed and configured your system as described in the *Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*.

How This Book Is Organized

This guide contains instructions about administering and using the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System.

Chapter 1 provides an overview of the Web Administrator software features.

Chapter 2 describes basic network and file system configuration.

Chapter 3 describes file system setup and management.

Chapter 4 describes system management functions.

Chapter 5 describes port settings.

Chapter 6 describes naming conventions.

Chapter 7 describes group, host, and file directory security settings.

Chapter 8 describes shares, quotas, and exports.

Chapter 9 describes licensable software options.

Chapter 10 describes monitoring functions.

Chapter 11 describes maintenance functions.

Chapter 12 contains removal and replacement procedures for customer-replaceable units (CRUs).

Appendix A contains instructions on using the console to perform system tasks.

Appendix B describes error messages that could be generated.

Appendix C details the Compliance Archiving Software API.

Appendix D contains system hardware details.

Appendix E describes how to send a diagnostic email.

Appendix F describes the panels in the Web Administrator graphical user interface.

Typographic Conventions

Typeface*	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen computer output	`% su` `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this. To delete a file, type `rm` *filename*.

* The settings on your browser might differ from these settings.

Related Documentation

The documents listed as online are available at:

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

Application	Title	Part Number	Format	Location
Safety	*Sun StorageTek 5320 NAS Server Regulatory and Safety Compliance Manual*	819-4281-*nn*	PDF HTML	Online
Safety	*Sun StorEdge 5300 RAID Expansion Unit and Sun StorEdge 5300 Expansion Unit Safety and Compliance Guide*	819-0882-*nn*	PDF	Online
Installation and known problems	*Sun StorageTek 5000 Family NAS Software Release Notes*	819-6402-*nn*	PDF HTML	Online

Application	Title	Part Number	Format	Location
Installation	*Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*	819-6387-*nn*	PDF HTML	Online
NAS Appliance Installation	*Sun StorageTek 5320 NAS Appliance Setup (Poster)*	819-6229-*nn*	Printed PDF	Shipping kit Online
Gateway	*Sun StorageTek 5320 NAS Gateway System (Poster)*	819-4286-*nn*	Printed PDF	Shipping kit Online

Documentation, Support, and Training

Sun Function	URL
Documentation	`http://www.sun.com/documentation/`
Support	`http://www.sun.com/support/`
Training	`http://www.sun.com/training/`

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to

`http://www.sun.com/hwdocs/feedback`

Please include the title and part number of your document with your feedback:

Sun StorageTek 5320 NAS Appliance and Gateway System Administration Guide, part number 819-6388-10

CHAPTER 1

Product Overview

This chapter provides an overview of the Sun StorageTek™ 5320 NAS Web Administrator graphical user interface. It includes the following sections:

Introduction

The Web Administrator graphical user interface (GUI) for the Sun StorageTek™ 5320 NAS Appliance systems makes it easy to set security and network configurations, and to perform administrative tasks on Sun Microsystems innovative Sun StorageTek 5320 NAS Appliance systems.

Note: Most software features and functions described in this book apply to any configuration of the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System software, in which case the general term "system" is used. Where a feature or function is limited to one of the configurations, that configuration is named specifically.

Using Web Administrator

The Web Administrator graphical user interface (GUI) enables you to configure system parameters through a series of menus and tab screens, or panels.These tab screens and settings are discussed in later chapters.

This section describes the interface layout and how to use the Web Administrator online help. The following subsections are included:

Logging In

The Login panel enables authorized users to access the system through the Web Administrator graphical user interface (GUI). By default, there is no password for the system administrator.

If you want to set a system administrator password, follow the directions in "Setting the Administrator Password" on page 61.

To log into the Web Administrator GUI:

1. Type the system administrator password in the Password field.

   Passwords are case-sensitive. If there is no system administrator password, leave this field blank.

2. Click Apply.

About the Interface Layout

The Web Administrator graphical user interface (GUI) is divided into the sections shown in the following figure.

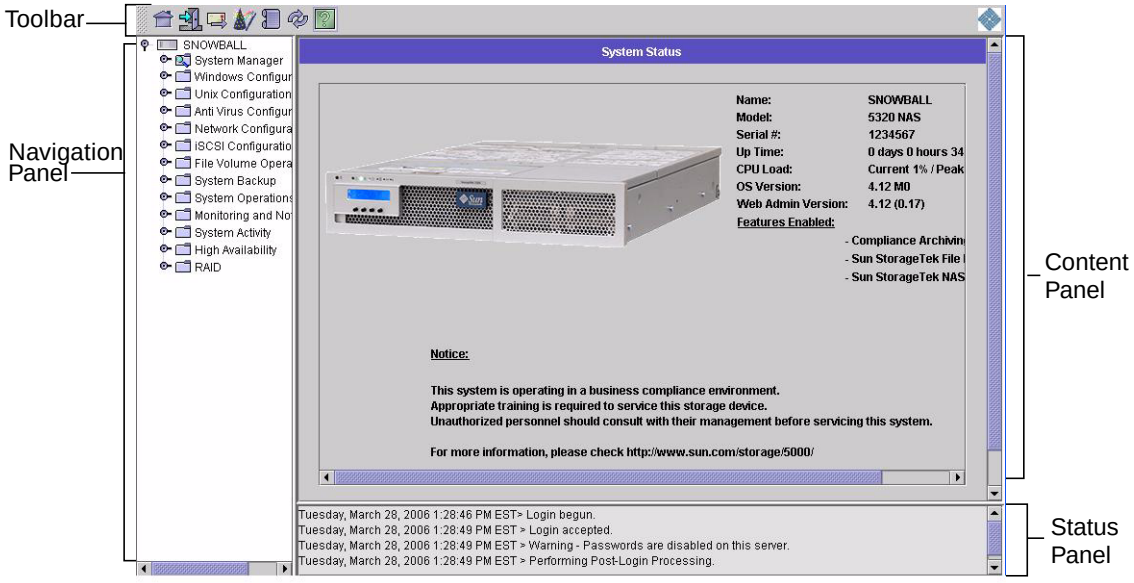


FIGURE 1-1 Main Window

The content displayed in the Web Administrator GUI varies based on your hardware configuration.

About the Toolbar

The toolbar, shown in the following figure, is displayed at the top of the Web Administrator graphical user interface (GUI).

FIGURE 1-2 Toolbar

The toolbar icons are shown in TABLE 1-1.

TABLE 1-1 Toolbar Icons

Button	Name	Action
	Home	View the home status screen.
	Log out	Log out of the software.
	Email	Send a diagnostic email.
	Wizard	Run the configuration wizard.
	System log	Access the system log.
	Refresh	Refresh the current panel and the Navigation panel.
	Help	Launch help in a separate window.

About the Navigation Panel

The navigation panel, shown in the following figure, enables you to navigate through the Web Administrator graphical user interface (GUI). You can access all configuration, setup, and administrative functions through this panel.

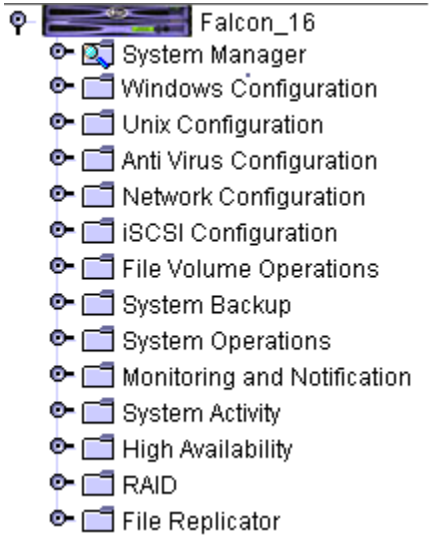


FIGURE 1-3 Navigation Panel

To open a folder, click the symbol next to the folder, or double-click the folder. The symbol changes to the position, as shown in the following figure.

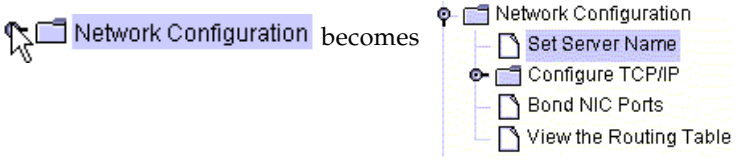


FIGURE 1-4 Expanding a Folder in the Navigation Panel

To close the folder, click the symbol back to the position.

About the Folder Symbol Key

Throughout the Web Administrator graphical user interface (GUI), folders are represented with symbols.The folder symbols are shown in TABLE 1-2.

TABLE 1-2 Folder Symbols

Symbol	Description
	File volume
	Compliant file volume (with red folder tab)
	Shared file volume
	Exported file volume
	Shared and exported file volume
	Mirrored file volume
	Compliant mirror
	Segment

About Other Buttons

Certain panels in the Web Administrator graphical user interface (GUI) contain other buttons. Additional buttons are shown in TABLE 1-3.

TABLE 1-3 Other Buttons

Button	Name	Action
	Add	Add an item.
	Up	Move the selected item up one level in the list.
	Down	Move the selected item down one level in the list.
	Trash	Delete the selected item.
	Edit	Edit the selected item.

About the Content Panel

The content panel, shown in the following figure, contains general information about the system.

FIGURE 1-5 Content Panel

For information about system status, see “Viewing System Status” on page 145.

About the Status Panel

At the bottom of the Web Administrator graphical user interface (GUI), the status panel displays all events that have occurred since the last logged in session. Use this panel to verify that your changes were saved or your system commands have run successfully. Errors and warnings are also displayed in this panel.

The following figure shows the status panel.

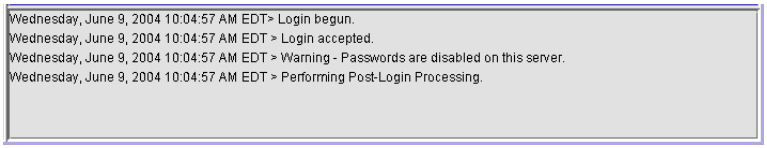


FIGURE 1-6 Status Panel

Note: The status panel displays the date and time for the client machine running the Web Administrator software, not the system's date and time.

Using Help

To view information about the Web Administrator software, click the Help button in the toolbar of the Web Administrator graphical user interface (GUI).

Note: If you have a pop-up blocker enabled on a Microsoft Windows system, you must disable the pop-up blocker to allow the help window to be displayed.

Information about the current panel is displayed in a help window. The help window consists of a navigation pane on the left and a topic pane on the right.

Click Help Contents to view all available topics. The left panel has a Contents and Index tab. Click a topic in the Contents or Index to view information about the selected topic.

Using the Configuration Wizard

The configuration wizard runs automatically the first time you log in to the Web Administrator software. The wizard is designed to guide you through the initial setup of your system. It helps you complete all of the steps necessary to establish communication between the system and your network. Once you complete the wizard, you still need to set up your file system and configure user access.

About Configuration Wizard Variations

The configuration wizard offers several options. Some of these options are automatically determined by the system itself. Other options are determined by you, based on the network environment you are running. This guide cannot cover all of the configurations in the available space. This section provides an overview of the configuration wizard itself and describes the possible paths you can take through the wizard.

Other functions and features also vary based on the features of the system. These variations are discussed in the appropriate locations within this guide.

There are three primary paths that the wizard can take. These three paths are based on the network environment you are running and you must choose the path in the wizard. These three paths are as follows:

- **UNIX only –** This path helps you configure the system for operation in a pure UNIX® network. It skips over all Windows-dependent features and functions.
- **Windows only –** This path helps you configure the system for operation in a pure Windows network. It skips over all UNIX–dependent features and functions.
- **Both UNIX and Windows –** This path combines all functions and features, helping you configure the system for a mixed network environment combining Windows and UNIX features.

On the first screen of the wizard, you must select the path appropriate to your network environment.

Running the Wizard

To run the configuration wizard:

1. Click the Wizard button () on the toolbar.

   The wizard is launched in a separate window.

2. Choose the path that you want to take and click Next.

   The wizard progresses through several steps, which are described in more detail in “Initial Network Configuration” on page 13. The steps are as follows:

   - Setting the server name and contact information
   - Configuring network adapters
   - Setting the default gateway

- Configuring Domains and Workgroups (Windows environments and mixed environments) and enabling and configuring Active Directory Service (ADS) (Windows environments and mixed environments)
- Configuring Windows Internet Naming Service (WINS) (Windows environments and mixed environments)
- Setting up Domain Name Service (DNS)

  Note: If the system started up using Dynamic Host Configuration Protocol (DHCP), confirm that the address of the DNS server is correct. If not, clear the Configure DNS checkbox to avoid delays in restarts and failovers.
- Setting up Network Information Service (NIS) (UNIX environments and mixed environments)
- Setting up Network Information Service Plus (NIS+) (UNIX environments and mixed environments)
- Configuring name services (UNIX environments and mixed environments)
- Setting up email notification
- Setting up remote and local logging
- Assigning the language

3. Review your settings and click Finish on the last screen of the wizard.

   The wizard saves your settings and lets you know if any configuration changes failed.

If you do not want to run the wizard, "Initial Network Configuration" on page 13 describes accessing the same functions in the same sequence through the navigation panel.

Where to Go From Here

Assuming you have initially configured your system by running the configuration wizard, the system is up and running and you have a basic understanding of how to navigate through the Web Administrator graphical user interface (GUI). From here you need to establish your file system and configure user access.

Establishing your file system includes defining any LUNs, partitions, file volumes, and segments that you need to set. For more information about these concepts, see "File System Concepts" on page 37.

When your file system is complete, you must set up user access rights and any other system management features. "System Management" on page 61 covers the basic management functions. View the index to find any specific features, including descriptions of the features, how they work, when and why they apply, and any specific rules for setting them up.

CHAPTER 2

Initial Network Configuration

This chapter describes configuring your system for communication on your network. It includes the following sections:

About the Initial Network Configuration

After you configure network communication and services, you need to configure your file system, user access rights, any other features, and any options that you purchased.

This chapter follows the same sequence as the configuration wizard. This documentation does not cover all of the features you might want to set up. If you want to set up a specific feature that is not covered in this chapter, look it up in the index to find the instructions.

Setting the Server Name

In order to configure your system for communication, you must set up a server name that identifies the server on the network.

To set the server name:

1. In the navigation panel, select Network Configuration > Set Server Name.
2. Type the server name in the Server Name field.

   The server name identifies the system or identifies the server unit, for dual-server high-availability (HA) systems on the network. The server name can include alphanumeric characters (a–z, A–Z, 0–9), "-" (dashes), "_" (underscores), and "." (periods).

   Note: The server name must begin with a letter (a–z or A–Z), not a number or a symbol. For example, "Astro2" and "Saturn_05" are acceptable server names. However "5Saturn" and "_Astro2" are not.
3. Type the contact information for your company.

   The system includes this information in any diagnostic email messages sent. For more information about diagnostic email messages, see "Sending a Diagnostic Email Message" on page 303.
4. Click Apply to save your settings.

Managing LUN Paths

This section provides information about logical unit numbers (LUNs) and how to set and restore LUN paths. The following subsections are included:

About Setting LUN Paths

A logical unit number (LUN) path is a designation that describes how a file volume in a LUN is accessed by which NAS server and controller. To every file volume there are two LUN paths from the NAS head controllers to the disk array controllers: primary and alternate. If one fails, the system automatically uses the other available LUN path to access the desired file volume. The number of LUN paths and their implementations depend on the model and configuration of the system. In a Sun StorageTek 5320 NAS Cluster Appliance, a server (head) induces a head failover (see "Enabling Head Failover" on page 20) if both the primary and alternate paths fail.

For more information, see "Setting LUN Paths" on page 18.

About LUN Paths in Single Server Systems

The following illustration is a typical hardware configuration in a single server system.

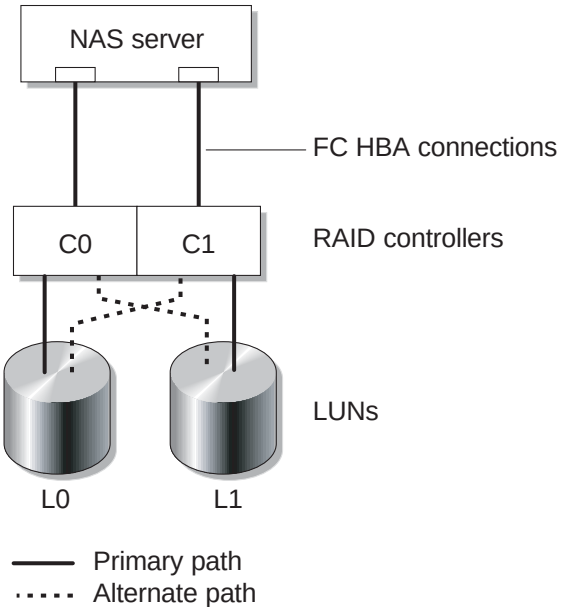


FIGURE 2-1 Single Server System Configuration

The primary LUN path to a file volume in LUN0 is C0-L0, and the alternate path is C1-L0. The primary LUN path to a volume in LUN1 is C1-L1, and the alternate path is C0-L1. As illustrated, the system has the following LUN paths.

TABLE 2-1 Primary and Alternate LUN Paths on a Single Server System

Paths	LUN0	LUN1
Primary	C0-L0	C1-L1
Alternate	C1-L0	C0-L1

Each LUN can be accessed through either controller 0 (C0) or controller 1 (C1).

About LUN Paths in Dual Server Systems

The following illustration is a typical hardware configuration in a Sun StorageTek 5320 NAS Cluster Appliance system.

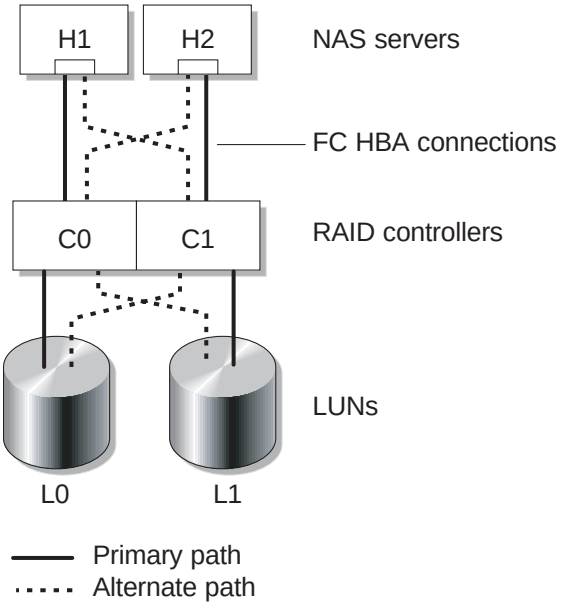


FIGURE 2-2 Dual Server System Configuration

The primary LUN0 path on Head 1 is C0-L0; the alternate path is C0-L1. The primary LUN0 path on Head 2 is C1-L0 and the alternate path is C1-L0.

File volumes are normally accessed through the primary LUN path designated for the LUN to which the file volumes belong. In a cluster configuration, a head induces a failover if its primary and alternate paths fail (see "Enabling Head Failover" on page 20).

Setting LUN Paths

By setting a logical unit number (LUN) path, you designate the current active LUN path. The current active LUN path can be either the primary or alternate path. For optimal performance, set the active path to the primary path. A LUN can be reassigned only if there are no file systems on that LUN. On a Sun StorageTek 5320 NAS Cluster Appliance system, only the server that "owns" a LUN can reassign it to another server.

Note: On a Sun StorageTek 5320 NAS Cluster Appliance system, when you first start the system, all LUNs are assigned to one server (H1). You must use server H1 to reassign some LUNs to server H2 for even distribution.

You use the Set LUN Path panel to set active paths. In a Sun StorageTek 5320 NAS Cluster Appliance system you can set an unassigned path from any server.

You can specify the primary and alternate path for each LUN or you can choose to automatically assign all LUN paths. If you want the LUN paths autoassigned, click the Auto-assign LUN paths button in the Set LUN Paths window.

To set a LUN path:

1. In the navigation panel, select High Availability > Set LUN Path.

   Note: LUNs that have no LUN path assigned might initially appear multiple times in the Set LUN Path panel, as their presence is advertised by multiple controllers over multiple paths. Once a LUN has a path assigned, it is displayed once, on its current path.

2. Select a LUN and click Edit.

3. Choose the controller that you want from the Primary Path drop-down menu.

   Example: The drop-down option "1/0" assigns the selected LUN to controller 0 (C0). The option value is *X*/*Y*, where *X* is the HBA and *Y* is the controller ID (SID) through which the LUN is seen by the NAS server. The "X" value is either 0 or 1. 1 designates that the controller is active, and 0 is inactive.

4. Evenly divide LUN assignments to the two available paths. For example, the first and third LUN to 1/0 and the second and fourth LUN to 1/1.

5. Click Apply.

Restoring a LUN Path

The current active path of a logical unit number (LUN) can be different from its primary path. The Restore option on the Set LUN Panel enables you to restore a current active path of a LUN to its primary LUN path.

Note: Restoring a LUN path does not recover any data; it is not a disaster recovery function. Instead, for optimal performance, the active path must be the primary path for a LUN.

To restore a LUN path:

1. In the navigation panel, select High Availability > Set LUN Path.
2. Select the LUN that you want to restore.
3. Click Restore.

Enabling Failover

This section provides information about enabling failover. The following subsections are included:

About Enabling Failover

Note: Enabling failover is only valid for Sun StorageTek 5320 NAS Cluster Appliance systems.

A Sun StorageTek 5320 NAS Cluster Appliance system consists of a pair of active-active servers, also called "heads," that share access to the redundant array of independent disks (RAID) controllers and several different networks. The RAID controllers are connected to each server through fibre controllers. A dedicated heartbeat cable connects the first network interface card (NIC) between the two servers and lets each server monitor the other's health status.

In normal operation, each server operates independently, with responsibility for a subset of logical unit numbers (LUNs). If one server suffers a hardware failure that renders a data path unavailable, the working server automatically takes ownership of Internet Protocol (IP) addresses and LUNs formerly managed by the failed server. All operations of the failed server, including RAID volume ownership and network interface addressing, are transferred to the working server. This is known as "head failover."

Note: Volume names must be unique in a cluster configuration. If two volumes in a cluster have the same name and a failover occurs, an 'x' will be appended to filesystem of the failed head to avoid a conflict with the working server.

Following a cluster failover, client operations using network file system/user datagram protocol (NFS/UDP) transfer immediately, while network file system/transmission control portal (NFS/TCP) requires a reconnect, which is performed transparently in the context of an NFS retry. Common internet file system (CIFS) also requires a reconnect, although different applications might do so transparently, notify the user, or require user confirmation before proceeding.

You can initiate the recovery process, known as "failback," when the failed head is repaired and brought back online. Using the Recover panel, accessible through High Availability > Recover, determine which LUNs are managed by which head.

Note: A power cycle (or power failure) of a single controller unit in a cluster configuration causes both heads to reset. This is expected behavior because each head is designed to protect against partial volume loss.

Enabling Head Failover

In the event of a head failure, failover causes the working head to take temporary ownership of the Internet Protocol (IP) addresses and logical unit numbers (LUNs) formerly managed by the failed head.

Note: When you enable head failover, Dynamic Host Configuration Protocol (DHCP) is automatically disabled.

To enable head failover:

1. In the navigation panel, select High Availability > Enable Failover.
2. Click the Automatic Failover checkbox.
3. Select the Enable Link Failover checkbox.

Enabling link failover ensures that head failover occurs when any network interface that is assigned a "primary" role fails. This type of failure is referred to as a "link down" condition. If the partner's network link is down, the head that wants to induce the failover must wait the specified amount of time after the partner head reestablishes its network link.

4. Enter the following:
   - **Down Timeout** – This is the number of seconds a head waits, in the event that the network link on one head becomes unreliable and the network link on its partner head is healthy, before inducing head failover.
   - **Restore Timeout** – This is the number of seconds the partner head's primary link must be up in order for the failover to take place. The Restore Timeout is used only when a link down induced failover is initiated but aborted due to the partner head's primary link being down.
5. Click Apply to save your settings.
6. Reboot both heads.

Initiating Failback (Recovery)

This section provides information about manually initiating failback (recovery) in the event that a failed head or redundant array of independent disks (RAID) controller is brought back online. The following subsections are included:

About Initiating Failback

When a failed head is brought back online, you must manually initiate recovery (failback) of your Sun StorageTek 5320 NAS Appliance or Sun StorageTek 5320 NAS Cluster Appliance system after it has undergone head failover.

A server that had failed and caused the failover to take place can "recover" its ownership of its original file volumes once the server is fully functional.

For example, volume A was assigned to server H1, which had failed, so server H2 took ownership of volume A during the failover. Now that server H1 is fully functional again, it can recover its ownership of volume A from server H2.

Caution: Make sure that the failed server is fully operable before attempting recovery.

Initiating Recovery

When a failed head is brought back online, you must manually initiate recovery (failback) of your Sun StorageTek 5320 NAS Appliance or Sun StorageTek 5320 NAS Cluster Appliance system after the system has undergone head failover.

To initiate recovery:

1. In the navigation panel, select High Availability > Recover.

   The Recover panel is displayed.

2. For head recovery, in the RAID list, select the RAID set you are recovering.
   - The Head 1 list identifies LUN mapping for server H1.
   - The Head 2 (partner) list identifies LUN mapping for the partner server H2.

3. Click Recover.

   The server rearranges the LUN mapping to reflect the configuration shown on the screen.

Configuring Network Ports and Adapters

This section provides information about configuring network ports and adapters. The following subsections are included:

About Configuring Network Ports

You can either enable Dynamic Host Configuration Protocol (DHCP) or specify the Internet Protocol (IP) address, netmask, broadcast, and network interface card (NIC) port role for each network port through the Configure Network Adapters panel. You can also add alias IP addresses for each NIC port.

Note: Each Sun StorageTek 5320 NAS Cluster Appliance NIC port must have an assigned role.

You can bond two or more ports together to create a port bond. A port bond has higher bandwidth than the component ports assigned to it. More information and instructions for bonding network ports are provided in "About Port Bonding" on page 69.

About Sun StorageTek 5320 NAS Appliance Port Locations

The Sun StorageTek 5320 NAS Appliance identifies ports in a predefined order based on their type and their physical and logical location on the server. To identify the network port locations for configuration, see "Back Panel Ports and LEDs" on page 293 and the *Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*. Note that system configurations vary and those shown are examples.

The relationship of network interface cards (NICs) to ports is also shown in the *Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*.

Configuring Network Adapters

To configure network adapters:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Configure Network Adapters.
2. If your network uses a Dynamic Host Configuration Protocol (DHCP) server to assign Internet Protocol (IP) addresses and you want to enable it, select the Enable DHCP checkbox.

Enabling DHCP allows the system to dynamically acquire an IP address from the DHCP server. Clear this checkbox to manually enter a static IP address and netmask. If you do not enable DHCP, the netmask is still disabled if the port is a member of an aggregate port. See "About Port Bonding" on page 69 for more information on creating and setting up aggregate ports.

Note: On Sun StorageTek 5320 NAS Cluster Appliance systems, you cannot enable DHCP unless you have disabled head failover. Instead, you must assign static IP addresses to ports so that they remain consistent in the event of a failover.

3. Select from the Adapter list the port you want to configure.

   If you have already created a port bond and want to add alias IP addresses to it, select the port bond from this list. (See "About Port Bonding" on page 69 for more information on creating port bonds.) Independent ports are labeled PORTx and port bonds are labeled BONDx.

   Once you create a port bond, you cannot add alias IP addresses to the individual ports, only to the bond.

4. Enter the IP address for the selected port or port bond.

5. Enter the netmask for the selected port or port bond.

   The netmask indicates which portion of an IP address identifies the network address and which portion identifies the host address.

   The read-only Broadcast field is filled automatically when you enter the IP address and netmask. The broadcast address is the IP address used to send broadcast messages to the subnet.

6. Select one of the following roles for each port.

Roles	Description
Primary	The port role of Primary identifies an active network port.
Independent	The port role of Independent identifies an active network port used for purposes other than serving data, such as backup.
Mirror	The port role of Mirror shows that the port connects this server to another server to mirror file volumes.
Private– Sun StorageTek 5320 NAS Cluster Appliance only	The Private port is reserved for the heartbeat, a dedicated network link that constantly monitors the status of the other head. Each head has only one private port.

Note: At least one port must be assigned a primary role.

For more details about port roles, see "About Port Bonding" on page 69.

7. To add an alias IP address to the selected port, enter it in the IP-Aliases field. Then click the Add button to add it to the IP-Aliases list.

   You can have up to nine aliases per interface for single-head systems and up to four aliases for dual-head systems. To remove an alias from the list, select it and click the Trash button. Changes are not saved until you click Apply.

8. Repeat Steps 3-7 for all ports in the Adapter list.

9. Click Apply to save your changes.

Setting the Default Gateway Address

The default gateway address is the Internet Protocol (IP) address of the gateway or router on the local subnet that is used by default to connect to other subnets. A gateway or a router is a device that sends data to remote destinations. You must specify the default gateway address for the system.

To set the default gateway address:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Set Gateway Address.

2. Enter the gateway address in the Gateway text box.

3. Click Apply to save your settings.

Managing Name Services

This section provides information about setting up Windows security so that name services can be used, and provides information about setting up various name services. For more detailed information about name services, see “Active Directory Service and Authentication” on page 75, “Active Directory Service and Authentication” on page 75. The following subsections are included:

Configuring Windows Security

To use name services in a Windows environment, you must configure Windows security. Configuring the domain, workgroup, or Active Directory Service (ADS) is a Windows function. If you are running a pure UNIX network, you do not need to configure either Windows Domains or Windows Workgroups.

Changing the security mode requires a server reboot. Therefore, you should perform this procedure during a scheduled maitenance period.

Enable Windows Workgroup, NT Domain security, or ADS through the Configure Domains and Workgroups panel. By default, your system is configured in Windows Workgroup mode, with a workgroup name of "workgroup."

Note – Domain security and Workgroup security settings are mutually exclusive. Changes made to Domain security will negate Workgroup security and vice versa.

To configure Windows security:

1. In the navigation panel, select Windows Configuration > Configure Domains and Workgroups.
2. To enable Windows domain security, select the Domain option and fill in the Domain, User Name, and Password fields. For more information about these fields, click Help on the panel, or see "Configure Domains and Workgroups Panel" on page 397.

   This option creates an account on the domain for this server. You must specify a user account with rights to add servers to the specified domain.
3. To enable Windows workgroup security, select the Workgroup option, and enter the name of the workgroup in the Name field.

   The workgroup name must conform to the 15-character NetBIOS limitation.
4. (Optional) In the Comments field, enter a description of the Sun StorageTek 5320 NAS Appliance system.
5. To enable ADS, select the Enable ADS checkbox and fill in the ADS-related fields. For more information about these fields, click Help on the panel, or see "Configure Domains and Workgroups Panel" on page 397.

   For more detail about ADS, refer to "About Active Directory Service" on page 76.

   Note: Prior to enabling ADS, you must verify that the system time is within five minutes of any ADS Windows domain controller. To verify the time, select System Operations > Set Time and Date from the navigation panel.

6. Click Apply to save your settings.

   If you change the security mode from workgroup to NT domain, or vice versa, the server automatically reboots when you click Apply.

Setting Up WINS

Windows Internet Naming Service (WINS) is a Windows function. If you are running a pure UNIX network, you do not need to set up WINS.

To set up WINS:

1. In the navigation panel, select Windows Configuration > Set Up WINS.
2. To enable WINS, select the Enable WINS checkbox.

   Checking this box makes the system a WINS client.
3. Type the Internet Protocol (IP) address of the Primary WINS server in the space provided.

   The primary WINS server is the server consulted first for NetBIOS name resolution.
4. Enter the Secondary WINS server in the space provided.

   If the primary WINS server does not respond, the system consults the secondary WINS server.
5. (Optional) Enter the NetBIOS Scope identifier in the Scope field.

   Defining a scope prevents this computer from communicating with any systems that do not have the same scope configured. Therefore, caution should be used with this setting. The scope is useful if you want to divide a large Windows workgroup into smaller groups. If you use a scope, the scope ID must follow NetBIOS name conventions or domain name conventions and is limited to 16 characters.
6. Click Apply to save your settings.

Setting Up DNS

Domain Name Service (DNS) software resolves host names to Internet Protocol (IP) addresses for your Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System.

Note: If you are using DNS without Dynamic DNS, add the host name and IP address of the server to your DNS database. If you are using Dynamic DNS, you do not need to manually update the DNS database. See your DNS documentation for more information.

To set up DNS:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Set Up DNS.
2. Select the Enable DNS checkbox.
3. Type the DNS server Domain Name.
4. Type the IP address of a DNS server you want to make available to the network, and then click the Add button to add the server to the Server List.

   Repeat this step for each DNS server you want to add. You can add a maximum of two DNS servers to this list.

   The system first queries the DNS server at the top of the server list for domain name resolution. If that server cannot resolve the request, the query goes to the next server on the list.
5. To rearrange the search order of the DNS servers in the list, click on the server you want to move and click the Up or Down button.

   To remove a server from the list, select the server IP address and click the Trash button.
6. Select the Enable Dynamic DNS checkbox to let a Dynamic DNS client add the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System into the DNS namespace.

   Do not enable this option if your DNS server does not accept dynamic updates. You must also configure the Kerberos realm and KDC server in “Configuring Windows Security” on page 26. If you enable Dynamic DNS by selecting this checkbox, nonsecure dynamic updates occur automatically if they are allowed by the DNS server.

7. To enable secure Dynamic DNS updates, select the Enable Dynamic DNS checkbox and fill in the DynDNS User Name and DynDNS Password fields. For more information about these fields, click Help on the panel, or see "Set Up DNS Panel" on page 355.

8. Click Apply to save your settings.

Setting Up NIS

Network information service (NIS) is a UNIX function. If you are running a pure Windows network, you do not need to set up NIS.

Use the Set Up NIS panel to enable NIS and specify the domain name and server Internet Protocol (IP) address.

To set up NIS:

1. In the navigation panel, select UNIX Configuration > Set Up NIS.

2. Select the Enable NIS checkbox.

   Enabling NIS configures the system to import the NIS database for host, user, and group information.

3. Type the name of the domain you want to use for NIS services in the Domain Name field.

   Use the DNS naming convention, for example, domain.com.

4. Type the IP address or name of the NIS server in the Server field.

   This is the server from which the database is imported.

   Leave the Server field blank if you do not know the server IP address. However, if you leave the Server field blank, you must select the Use Broadcast checkbox. Use Broadcast automatically acquires the appropriate IP address of the NIS server.

5. Enter the frequency rate, in minutes, you want NIS information to be refreshed. The default is set to 5 minutes.

6. Select the Use Broadcast checkbox to automatically acquire the NIS server IP address.

7. Select the Update Hosts checkbox to download host information from the NIS server to the system.

8. Select the Update Users checkbox to download user information from the NIS server to the system.

9. Select the Update Groups checkbox to download group information from the NIS server to the system.
10. Select the Update Netgroups checkbox to download netgroup information from the NIS server to the system.
11. Click Apply to save your changes.

Setting Up NIS+

Network information services plus (NIS+) is a UNIX function. If you are running a pure Windows network, you do not need to set up NIS+.

Note: There is no relation between NIS+ and NIS. The commands and structure of NIS+ are different from NIS.

There are two steps involved in setting up NIS+:

1. Adding the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System to the host credential file on the NIS+ server.
2. Configuring NIS+.

To add the Sun StorageTek system to the host credential file on the NIS + server:

1. Log in as `root`.
2. Type the following command:

   `nisaddcred -p unix.`*`server`***`@`***`domain`** **`-P`** *`server`***`.`***`domain`***`. des`**

   where *server* is the name of the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, and *domain* is the name of the NIS+ domain that the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System is joining.

   Note: You must add a period to the end of the domain name only after the **`-P`** argument.

   For example, if the Sun StorageTek 5320 NAS Appliance is named **SS1**, and its NIS+ domain is sun.com, enter:

   `nisaddcred -p unix.ss1@sun.com -P ss1.sun.com. des`

3. At the prompt, enter a password.

This password is also used later in this procedure for configuring the system to use NIS+. Enter the password.

To configure NIS+:

1. From a remote client, open a web browser window to the system and log in to Web Administrator.
2. In the navigation panel, select UNIX Configuration > Set Up NIS+.
3. Select the Enable NIS+ checkbox.
4. In the Home Domain Server field, enter the NIS+ home domain server IP address.

   If you don't know the home domain server IP address, leave this field blank and select the Use Broadcast checkbox. When this option is selected, the system automatically acquires the appropriate IP address for the home domain server.
5. In the NIS+ Domain field, enter the NIS+ home domain.

   Note: NIS+ domain names must end with a period (".").
6. Enter the secure RPC password for the NIS+ server.

   This is the password that was set during Step 13. on page 30.
7. Enter the search path as a colon-separated list of domains.

   The search path identifies the domains that NIS+ searches through when looking for information. Leave this space empty to search only the home domain and its parents.

   For example, if the NIS+ domain is `eng.sun.com.` and the search path is blank, the system first searches `eng.sun.com.` then `sun.com.`, and so on, when resolving names. Conversely, if you specify a search path like `sun.com.`, the system searches only the domain `sun.com` when resolving names.
8. Select the Use Broadcast checkbox if you do not know the IP address of the home domain server (see step 5).
9. Click Apply to save your settings.

Configuring Name Services

The name service (NS) lookup order controls the sequence in which the name services are searched to resolve a query. These name services can include LDAP, NIS, NIS+, DNS, and Local. You must enable the selected services to use them for name resolution.

To set the order for user, group, netgroup, and host lookup:

1. In the navigation panel, select UNIX Configuration > Configure Name Services.
2. Select the order of user lookup in the Users Order tab by selecting a service from the Services Not Selected box and using the > and < buttons, and then use the Up and Down buttons in the Services Selected box.
3. Select the services used for group lookup in the Groups Order tab, following the procedure in step 2.
4. Select the services used for netgroup lookup in the Netgroup Order tab, following the procedure in step 2.
5. Select the services used for host lookup in the Hosts Order tab, following the procedure in step 2.
6. Click Apply to save your changes.

Setting Up Email Notifications

Set the Simple Mail Transfer Protocol (SMTP) server name and email notification recipients in this screen. When the system detects an error, it sends a notification email message.

In order to ensure name resolution, you must have either set up the SMTP server host name in the Configure Hosts panel (see "About Configuring Hosts" on page 88) or set up DNS (see "Setting Up DNS" on page 28).

To set up SMTP and send email messages to the recipients:

1. In the navigation panel, select Monitoring and Notification > Set Up Email Notification.
2. Type the name of the SMTP server that you want to use to send notification.
3. Type the email address of a person that you want to automatically notify of system errors in the Email Address box.
4. Specify the types of email for this recipient. Select Notification, Diagnostics, or both.
5. Click the Add button to add the new recipient to the List of recipients.
6. Repeat Step 3 through Step 5 for all recipients. You can enter a maximum of four email addresses.

   To remove someone from the list, select the address and click the Trash button.

7. Select the notification level.

8. Click Apply to save your settings.

Setting Up Logging

Enabling remote logging lets the system send its log to a designated server and/or save it to a local archive. The designated server must be a UNIX server running `syslogd`. If you will be referring to the logging host by domain name, you must configure the Domain Name Service (DNS) settings on the system before you enable remote logging.

Caution: You must enable remote logging or create a log file on local disk to prevent the log from disappearing on system shutdown. Otherwise, the system will create a temporary log file in volatile memory during startup. This is sufficient to retain any errors that might occur during initial startup for later display, but will not persist through a power failure or system restart.

To set up remote and local logging:

1. In the navigation panel, select Monitoring and Notification > View System Events > Set Up Logging.

2. Select the Enable Remote Syslogd box.

3. In the Server field, enter the DNS host name if you have configured the DNS settings. Otherwise, enter the Internet Protocol (IP) address. This is where the system log is sent.

4. Select the appropriate facility.

   The facility indicates the application or system component generating the messages.

   Note: *All messages sent to the* `syslogd` *server will have this facility value.*

   The possible facility values in the Set Up Remote Logging panel are as described in the following table.

Facility	Description
Kern	Messages generated by the kernel. These cannot be generated by any user processes.
User	Messages generated by random user processes. This is the default facility identifier if none is specified.
Mail	The mail system.

Facility	Description
Daemon	System or network daemons.
Auth	Authorization systems, such as login.
Syslog	Messages generated internally by syslogd.
Local0–Local7	Reserved for local use.

5. Select the types of system events to be logged by placing a check mark on each (see "About System Events" on page 148).
6. To set up a local log, check Enable Local Log.
7. Enter the log file's path (the directory on the system where you want to store the log file) and file name in the Local File field.

   Note: You cannot set up local logging to the `/cvol` directory. Specify another directory such as `/dvol/error.txt`.
8. Enter the maximum number of archive files in the Archives field.

   The allowable range is from 1 to 9.
9. Type the maximum file size in kilobytes for each archive file in the Size field.

   The allowable range is from 100 to 999,999 kilobytes.
10. Click Apply to save your settings.

Assigning the Language

The operating system supports Unicode, which enables you to set the local language for network file system (NFS) and common internet file system (CIFS). Ordinarily, you assign the language when you run the wizard during initial system setup. However, if you need to reset the language at a later time, you can set it manually.

To assign the language:

1. In the navigation panel, select System Operations > Assign Language.
2. Select the local language for from the languages displayed in the pull-down menu.
3. Click Apply to save your changes.

Backing Up Configuration Information

After you have completed the system configuration, back up the configuration information in the event of a system failure. For information about backing up configuration information, see “Backing Up Configuration Information” on page 220.

Where to Go From Here

At this point, your system is in full communication with the network. However, before your users can begin storing data, you must set up the file system and establish user access rights. For more information, see “File System Setup and Management” on page 37.

To set up quotas, shares, exports, or other access controls, see “Shares, Quotas, and Exports” on page 103.

If there is a specific function you want to set up, look it up in the index to find the instructions.

CHAPTER 3

File System Setup and Management

This chapter covers file system concepts, setup, and management for the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance.

It includes the following sections:

File System Concepts

The following sections provide definitions of some of the basic file system concepts and attributes used in NAS storage:

About RAID Configurations

There are different RAID system configurations that are supported by the system. The following sections describe these configurations:

About RAID Systems

Redundant array of independent disks (RAID) systems allow data to be distributed to multiple drives through an array controller for greater performance, data security, and recoverability. The basic concept of a RAID system is to combine a group of smaller physical drives into what looks to the network as a single very large drive. From the perspective of the computer user, a RAID system looks exactly like a single drive. From the perspective of the system administrator, the physical component of the RAID system is a group of drives, but the RAID system itself can be administered as a single unit.

There are multiple types of RAID configurations. The Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance software support RAID 5 only. The Sun StorageTek 5320 NAS Gateway System software supports RAID 1, RAID 0+1, and RAID 5.

About the RAID 0 Configuration (Not Supported)

The RAID 0 configuration does not include the redundancy for which redundant array of independent disks (RAID) systems were developed. However, it provides a significant increase in drive performance. The RAID 0 configuration employs the concept of *striping*. Striping means that data is divided into stripes. One stripe is written to the first drive, the next to the second drive, and so on. The primary advantage of striping is the ability for all drives in the array to process reads and writes simultaneously. Simultaneous access greatly speeds both writes and reads.

However, because there is no redundancy in a RAID 0 configuration, if one drive fails, all of the data on the entire array may be lost. The RAID 0 configuration is best used in situations where performance is the overriding concern and lost data is of less significance.

About the RAID 1 Configuration (Sun StorageTek 5320 NAS Gateway System Only)

Drive *mirroring* is the primary concept of the redundant array of independent disks (RAID) 1 array, which doubles the number of drives required to provide the same amount of storage, but provides an up-to-date backup of the drive. The mirrored drive is always online and can be accessed very quickly if the primary drive fails. Each primary drive is mirrored by a second drive of the same size. All writes are duplicated and written to both members of the RAID 1 array simultaneously. The RAID 1 array provides excellent high availability. A RAID 1 array is most useful where data security and integrity are essential, but performance is not as significant.

About the RAID 0+1 Configuration (Sun StorageTek 5320 NAS Gateway System Only)

Redundant array of independent disks (RAID) 0+1 combines two RAID concepts to improve both performance and high availability: striping and mirroring. The mirrored drive pairs are built into a RAID 0 array. All writes are duplicated and written to both mirrored drives simultaneously. The striping of the RAID 0 improves performance for the array as a whole, while drive mirroring (RAID 1) provides excellent high availability for each individual drive. RAID 0+1 is a good choice for environments where security may outweigh performance, but performance is still important.

About the RAID 5 Configuration

The redundant array of independent disks (RAID) 5 array claims the best of both the performance improvements of striping and the redundancy of mirroring, without the expense of doubling the number of drives in the overall array.

RAID 5 uses striping and *parity* information. Parity information is data created by combining the bits in the information to be stored and creating a small amount of data from which the rest of the information can be extracted. In other words, the parity information repeats the original data in such a way that if part of the original is lost, combining the remainder of the original and the parity data reproduces the

complete original. The parity information is not stored on a specific drive. Instead, a different drive in the stripe set is used for parity protection for different regions of the RAID 5 set.

The RAID 5 array includes the parity information as one of the stripes in the stripe arrangement. If one drive in the array fails, the parity information and the remaining portion of the original data from the surviving drives are used to rebuild the now missing information from the failed drive. Thus the RAID 5 array combines the high availability of the mirror with the performance of the stripes and produces the best overall RAID type. It also has the advantage of requiring very little "extra" space for the parity information, making it a less expensive solution as well.

The first enclosure with drives in each array (the 5300 RAID EU for Fibre Channel arrays or the first EU S attached to the empty 5300 RAID EU for SATA arrays) contains two 6-drive (5+1) RAID 5 groups plus two global hot spares. All subsequent EU F or EU S enclosures contain either one or two 7-drive (6+1) RAID 5 groups for a total of 7 or 14 drives.

Caution: Do not update system software or RAID firmware when the RAID subsystem is in critical state, creating a new volume, or rebuilding an existing one.

About LUNs

A logical unit number (LUN) identifies the logical representation of a physical or virtual device. In the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance, there is a one-to-one correspondence between RAID sets and LUNs. However, the system manages LUNs as independent entities and treats the LUN as a single storage volume.

By treating LUNs this way, the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance greatly simplify the process of establishing a file system. The space on the RAID set is accessed independently of the physical drive limits through the LUN.

Management of the storage resources is accomplished through the LUN, with little direct management of the RAID sets themselves. See "About Creating RAID Sets and LUNs" on page 43 for directions and more information on setting up both RAID sets and LUNs.

About Partitions

Partitions are sections on a logical unit number (LUN) and provide a way to subdivide the total space available within a LUN. The Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance operating systems support a maximum of 31 partitions per LUN.

When a LUN is first created, all of the available space is located in the first partition and any others are empty. To use the space in a partition, you must create a file volume. Each partition can contain only one file volume, though a single file volume can span several partitions. When you make a file volume, the size of the partition is automatically adjusted to match the size of the file volume. Any additional space on the LUN is automatically assigned to the next partition. Once you have made all of the file volumes the operating system supports, any extra space on that LUN is inaccessible.

You can increase the size of a file volume by attaching a segment (see "About Segments" on page 42). The segment is essentially another file volume with special characteristics. When you add a segment to an existing volume, the two become inseparable and the only thing the user sees is more space in the volume. The flexibility of this system enables you to create a file volume and then to expand it as needed without disturbing your users and without forcing them to spread their data over several volumes.

While the system administrator is adding drives and LUNs, all that the user sees is that there is more space within the volume.

About File Volumes

File volumes define the spaces that are available for storing information, and are created from partitions that have available space. If the volume does not use up all the available space in a partition, the remaining space is automatically allocated into the next partition. New file volumes are limited to 255 gigabyte in size. To create a larger file volume, you can create and attach up to 63 segments (see "About Segments" on page 42) to the original file volume.

From the user's point of view, the file volume and any directory structures within it are the focus. If the file volume begins to fill up, the administrator can attach another segment and increase the available space within that file volume. In physical terms,

this may involve adding more drives and even expansion enclosures. However, the physical aspect is invisible to the user. All the user sees is more storage space within the volume.

About Segments

Segments are "volumes" of storage space created much like file volumes. They can be attached to an existing file volume at any time. Attaching a segment increases the original file volume's total capacity. Each segment must be created independently and then attached to a file volume. Once attached to a file volume, the volume and the segment are inseparable.

In general, segments are created as needed and attached to volumes as the volumes begin to fill with data. The main advantage of adding space by attaching segments is that you can create the segment on a new drive or even a new array. Once the segment is attached to the original file volume, the different physical storage locations are invisible to the user. Therefore, space can be added as needed, without bringing down the network to restructure the data storage and create a bigger file volume.

Creating the File System

This section provides information about creating the Sun StorageTek file system. The following subsections are included:

About Creating the File System

If you are configuring a Sun StorageTek 5320 NAS Gateway System, use the storage system configuration tools to create hot spare drives and logical unit numbers (LUNs). Refer to the documentation supplied with the storage system that is connected to your gateway.

If you are configuring a Sun StorageTek 5320 NAS Appliance or Cluster system, refer to the sections “About Creating RAID Sets and LUNs” on page 43 and “Designating a Drive As a Hot Spare” on page 44.

About Creating RAID Sets and LUNs

The Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance combine the creation and definition of the redundant array of independent disks (RAID) set into the definition of the logical unit number (LUN). (See “File System Concepts” on page 37 for more information.) In effect, you create both objects simultaneously. The Sun StorageTek 5320 NAS Appliance and Cluster systems let you choose the basic structure of the RAID set and define the LUN, automating the many tasks usually associated with defining a RAID set.

Caution: Sun StorageTek 5320 NAS Cluster Appliance users: Each server manages its own LUNs. Before adding LUNs, be sure that failover has been enabled and configured. Refer to “About Enabling Failover” on page 19 for details.

The Sun StorageTek 5320 NAS Appliance and Cluster systems also automate the definition of partitions. Partitions are automatically defined when you create a LUN. Initially, the Sun StorageTek 5320 NAS Appliance and Cluster systems have two hot spare drives assigned and at least two default LUNs.

RAID sets and LUNs are created simultaneously in Sun StorageTek 5320 NAS Appliance and Cluster systems, simplifying the process of establishing both.

When adding a LUN, be sure that you have not assigned the disks in the LUN another function (for example, hot spare) prior to LUN creation. Any drive that has been assigned to another LUN or as a hot spare is not available for inclusion in a new LUN.

Adding a New LUN

To add a new logical unit number (LUN):

1. In the navigation panel, select RAID > Manage RAID.

   The Manage RAID Panel is displayed.

   Note: To locate a drive or drive tray, you can click on the Locate Drive or Locate Drive Tray button, which will cause the LCD indicator for the drive or drive tray to flash.

2. Click Add LUN.

   The Add LUN window is displayed.

3. From the RAID EU pull-down menu, select the number of the controller to which you want to add a LUN.

4. Select the drives that will belong to the LUN by clicking each drive image.

   You must select at least three drives. The drive images show the status of each drive. For information about the drive images and their statuses, see "Add LUN Window" on page 359.

5. Choose one of the following volume options, listed in the following table.

Option	Description
New Volume	Select this option to create a new volume for this LUN. The entire LUN will be used to create the volume. Type the name of the new volume in the space provided. **Note**: In a cluster configuration, volume names must be unique across cluster members.
Existing Volume	Select this option if the purpose of this LUN is to add disk space to an existing volume (to create and attach a segment). Then select the volume you are expanding from the pull-down menu.
None	Select this option to create a new LUN without assigning it a name.

6. Click Apply to add the new LUN.

   Allow several hours for the system to add the LUN.

Designating a Drive As a Hot Spare

You can configure a drive as a hot spare for the Sun StorageTek 5320 NAS Appliance or Cluster system.

To designate a drive as a hot spare:

1. In the navigation panel, select RAID > Manage RAID.

2. Click the Add HS button at the bottom of the screen.

3. Select the drive you want by clicking the drive image.

   Be sure that the disk you use as a hot spare is at least as large as the largest disk in any logical unit number (LUN) on this server.

The drive images show the status of each drive, as described in the following table.

Drive	Indication
	The drive in this slot is available as a hot spare.
	The drive in this slot has been selected as a hot spare.
	No drive is present in this slot.

4. Click Apply to add the new hot spare.

Creating File Volumes or Segments

This section provides information about creating file volumes or segments. The following subsections are included:

About Creating a File Volume or a Segment

New file volumes are limited to 255 gigabyte in size. To create a larger file volume, you can add up to 63 segments to the primary volume. If you want a larger file volume, create one primary volume and up to 63 segments. Then attach the segments to the primary volume to increase its size.

A file volume or segment can be created using the Create File Volumes panel or the System Manager.

Creating a File Volume or Segment Using the Create File Volumes Panel

To create a file volume or segment using the Create File Volumes panel:

1. In the navigation panel, select File Volume Operations > Create File Volumes.
2. If you have recently added new disks to the live system without performing a reboot, click the Scan For New Disks button.

   The partition number for the file volume in the Partition pull-down menu will automatically increment when the file volume is created.
3. Type in the name of the new volume or segment in the Name field.

   Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).

   Note: In a cluster configuration,volume names must be unique across cluster members. Identical volumes names cause problems in the event of failover. See "About Enabling Failover" on page 19 for more information.
4. Select whether the size of the file volume is reported in MB (megabytes) or GB (gigabytes) by clicking on the pull-down menu.
5. Type in the file volume size in whole numbers.

   The total space available is shown directly beneath this field.
6. Select the file volume type (Primary or Segment).

7. If you have the Compliance Archiving software installed and you want to create a compliance-enabled volume, click Enable in the Compliance section. Then specify the type of compliance enforcement that is needed.
   - If you select Mandatory Enforcement, the default retention time will be permanent. Administrative override is not permitted.

     Caution: Once you enable compliance archiving with mandatory enforcement on a volume, that volume cannot be deleted, be renamed, or have compliance archiving disabled or downgraded to advisory enforcement.
   - If you select Advisory Enforcement, the default retention time will be zero days. Administrative override is permitted.

     Note: Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See "Managing Trusted Hosts" on page 246.

     For more information, see "About Compliance Archiving Software" on page 136.
8. Click Apply to create the new file volume or segment.

Creating a File Volume or Segment Using the System Manager

To create a file volume or segment by using the System Manager:

1. Right-click System Manager in the navigation panel.
2. Choose Create Volume or Create Segment from the pop-up menu to open the desired window.
3. In the LUN box, click the logical unit number (LUN) on which you want to create the primary file volume.

   The partition number for the file volume in the Partition pull-down menu will automatically increment when the file volume is created.
4. Type in the name of the new volume or segment in the Name field.

   Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).
5. Select whether the size of the file volume is reported in MB (megabytes) or GB (gigabytes) by clicking on the pull-down menu.

6. Type in the file volume size in whole numbers.

   The total space available is shown directly beneath this field.

7. Select the file volume type (Primary or Segment).

8. If you have the Compliance Archiving software installed and you want to create a compliance-enabled volume, click Enable in the Compliance section. Then specify the type of compliance enforcement that is needed.

   - In you select Mandatory Enforcement, the default retention time will be permanent. Administrative override is not permitted.

     Caution: Once you enable compliance archiving with mandatory enforcement on a volume, that volume cannot be deleted, be renamed, or have compliance archiving disabled or downgraded to advisory enforcement.

   - If you select Advisory Enforcement, the default retention time will be zero days. Administrative override is permitted.

     Note: Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See "Managing Trusted Hosts" on page 246.

     For more information, see "About Compliance Archiving Software" on page 136.

9. Click Apply to create the new file volume or segment.

Attaching Segments to a Primary File Volume

This section provides information about attaching segments to a primary file volume. The following subsections are included:

About Attaching Segments to a Primary File Volume

Attaching segments to a primary file volume expands the size of the volume. The segment becomes permanently associated with the volume and cannot be removed. You must create a segment before you can attach it to a volume. Refer to "About Creating a File Volume or a Segment" on page 46 for instructions.

Caution: Attaching a segment to a primary file volume cannot be reversed.

A file volume by itself is limited to 255 gigabytes; however, up to 63 segments from any LUN can be attached to any file volume. Each segment can be as small as 8 megabytes and as large as 255 gigabytes.

A segment can be attached using the Attach Segments panel or the System Manager.

Caution: Compliance-enabled volumes with mandatory enforcement cannot be deleted. If you add a segment to a compliance-enabled volume with mandatory enforcement, you will not be able to delete or reclaim the space used by the segment.

Attaching a Segment Using the Attach Segments Panel

To attach a segment by using the Attach Segments panel:

1. Access the Attach Segments panel by clicking File Volume Operations > Attach Segments.
2. Click to select the desired volume from the Existing Volumes box.
3. Click to select the desired segment from the Available Segments box.
4. Click Apply to attach.

Attaching a Segment Using the System Manager

To attach a segment by using the System Manager software:

1. Click System Manager in the Navigation pane to view existing volumes.
2. Right-click the desired file volume to access the pop-up menu, and select Attach Segments.

3. For each segment that you want to attach, select the desired segment and click Apply to attach it.

   Only one segment can be selected and attached at a time.

About Rebuilding a LUN

If one of the drives in a logical unit number (LUN) fails, the light-emitting diode (LED) on that drive turns steady amber, indicating it is waiting to be replaced with a new drive.

Note: LUN rebuilding does not apply to Sun StorageTek 5320 NAS Gateway System system configurations.

If a hot spare drive is available, the redundant array of independent disks (RAID) set associated with the failed drive will be rebuilt using that hot spare. All drives associated with the rebuild will have LEDs blinking green and should not be removed during the rebuilding process. A similar rebuild will take place when the failed drive is replaced, as the new drive is reinserted into the RAID set and the hot spare is returned to standby mode. Rebuilding may take several hours to complete.

If your system does not include a hot spare, you must remove the failed drive and replace it with another drive of the same or larger capacity. See Appendix D for information on replacing a failed drive.

After you replace the faulty drive, the RAID controller automatically rebuilds the LUN. LUN rebuilding may take several hours, depending on disk capacity. The LUN drive LEDs blink amber during LUN rebuilding.

Managing File Volumes and Segments

File system management tasks include the following:

Editing File Volume Properties

You can change the properties of a file volume using the Edit Volume Properties panel.

Note: Compliance-enabled volumes with mandatory enforcement cannot be renamed or have compliance archiving disabled or downgraded to advisory enforcement.

To rename a volume, enable checkpoints, enable quotas, or edit compliance properties:

1. In the navigation panel, select File Volume Operations > Edit Properties.
2. Select the name of the volume you want to change from the Volumes list.
3. Enter the volume's new name (if applicable) in the New Name field.

   Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).
4. Select one of the options describe in the following table.

Option	Description
Enable Checkpoints	Select this checkbox to create checkpoints for the file volume. Checkpoints are enabled by default when you create a file volume.
Enable Quotas	Select this checkbox to enable quotas for the selected volume. Quotas are disabled by default when you create a file volume.
Enable Attic	Select this checkbox to temporarily save deleted files in the `.attic$` directory located at the root of each volume. By default, this option is enabled. In rare cases on very busy file systems, the `.attic$` directory can be filled faster than it processes deletes, leading to a lack of free space and slow performance. In such a case, you should disable the `.attic$` directory by deselecting this checkbox.

5. If the volume is compliance-enabled, you have several options in the Compliance Archiving Software section, as described in the following table, depending on the level of compliance enabled.

Caution: For compliance-enabled volumes with mandatory enforcement, the default retention time is "Permanent."For compliance-enabled volumes with advisory enforcement, the default retention time is zero days. If you want to set a

different default retention time, you must specify the new retention period *before* you begin using the volume.

Caution: Once you enable compliance archiving with mandatory enforcement on a volume, that volume cannot be deleted, be renamed, or have compliance archiving disabled or downgraded to advisory enforcement.

For more information, see "About Compliance Archiving Software" on page 136.

Option	Description
Mandatory Enforcement	If the volume is compliance-enabled with mandatory enforcement, you cannot change to advisory enforcement.
Advisory Enforcement	If the volume is compliance-enabled with advisory enforcement and you want to change the volume to be compliance-enabled with mandatory enforcement, you can change the setting by selecting Mandatory Enforcement.
Permanent Retention	Default. If you do not want the data permanently retained, you must select the Retain for *nn* Days option before you use the volume. Select this option to permanently retain the data on this volume.
Retain for *nn* Days	Select this option and use the drop-down menu to specify the number of days for which the data is to be retained. If the volume is compliance-enabled with advisory enforcement, you can increase or decrease the retention period. If the volume is compliance-enabled with mandatory enforcement, you can only increase the retention period.

6. Click Apply to save your changes.

Deleting File Volumes or Segments

In some instances, after deleting files, volume free space does not change, most likely due to the checkpoint feature or the attic enable feature. (For information about attic enabling, see "Editing File Volume Properties" on page 51.)

Checkpoints store deleted and changed data for a defined period of time to enable retrieval for data security. This means that the data is not removed from disk until the checkpoint is expired, a maximum of two weeks, except in the case of manual checkpoints, which can be kept indefinitely.

If you are deleting data to free disk space, you will need to remove or disable checkpoints. Refer to “Removing a Checkpoint” on page 167 for instructions on removing checkpoints.

Note: Compliance-enabled volumes with mandatory enforcement cannot be deleted, and volumes that are offline cannot be deleted.

To delete a file volume or segment:

1. In the navigation panel, select File Volume Operations > Delete File Volumes.
2. Select the file volume or segment you want to delete.
3. Click Apply.

Viewing Volume Partitions

The View Volume Partitions panel is a read-only display of the logical unit numbers (LUNs) defined for the Sun StorageTek 5320 NAS Appliance or Cluster system.

To view volume partitions:

1. In the navigation panel, select File Volume Operations > View Volume Partitions.
2. In the Volumes list, select the file volume for which you want to view partitions.

Configuring the iSCSI Protocol

This section provides information about configuring the Internet Small Computer Systems Interface (iSCSI) protocol. The following subsections are included:

About iSCSI Configuration

You can configure the system to use the Internet Small Computer Systems Interface (iSCSI) protocol to transport data from host applications to the Sun StorageTek 5320 NAS Appliance storage. iSCSI transports SCSI commands, data, and status over a network file system transmission control protocol/Internet Protocol (TCP/IP) network. When you enable iSCSI, host applications can store data on the Sun StorageTek 5320 NAS Appliance.

In an iSCSI environment, the Sun StorageTek 5320 NAS Appliance acts as the iSCSI target for an iSCSI initiator client. Each iSCSI initiator and target has a unique, permanent identifier. The iSCSI initiator identifier is generated by iSCSI software on the host. The iSCSI target supports both EUI (Enterprise Unique Identifier) and IQN (iSCSI Qualified Name) identifiers.

About Configuring an iSCSI Target

Configuring an Internet Small Computer Systems Interface (iSCSI) target to connect to and access an iSCSI target logical unit number (LUN) requires the following steps:

- Configure the iSCSI initiator client (see the documentation provided with the iSCSI initiator software)
- Create an access list to allow iSCSI initiator access to the target
- Create a LUN and assign iSCSI initiator access to the LUN
- Configure the iSCSI target and initiator discovery method

The iSCSI target implemented on the Sun StorageTek 5320 NAS Appliance is based on iSCSI RFC 3720 developed by the Internet Engineering Task Force (IETF). The supported protocol features include header digest, initiator Challenge Handshake Authentication Protocol (CHAP), and error recovery level 0.

About Configuring iSCSI Initiator Access

You can define which Internet Small Computer Systems Interface (iSCSI) initiators can access a logical unit number (LUN) by creating an iSCSI access list. An access list can include one or more iSCSI initiators, and optionally, a CHAP initiator and password. CHAP ensures that the data is sent from an authentic iSCSI initiator.

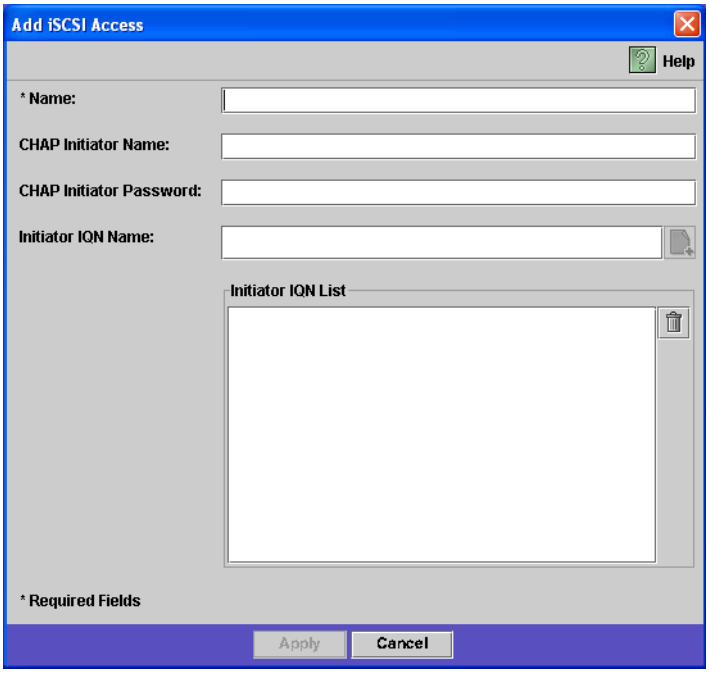
Caution: You can configure more than one iSCSI initiator to access the same iSCSI target LUN. However, an application (clustering or database) running on an iSCSI client server has to provide synchronized access to avoid data corruption.

Creating an iSCSI Access List

To create an Internet Small Computer Systems Interface (iSCSI) access list:

1. In the navigation pane, select iSCSI Configuration > Configure Access List.
2. To create an access list, click Add.

The Add iSCSI Access window is displayed.



3. Fill in the fields. For detailed information about the fields, click the Help button in the window, or see "Add/Edit iSCSI Access Window" on page 335.

4. Click Apply to save the settings.

   You can edit an iSCSI access list by double-clicking on one of the access list names, or by selecting an access list name and click Edit. Change any of the text fields and click Apply to save the settings.

About iSCSI Sparse LUNs

As a general rule when creating Internet Small Computer Systems Interface (iSCSI) logical unit numbers (LUNs), use non-sparse LUNs, as long as sufficient storage is available.

iSCSI sparse LUNs are not useful in all situations. If you create sparse LUNs, disk space is not allocated prior to use. Sparse LUNs are useful when you expect that several LUNs will be created that will not use their full capacity. For example, when

you expect that five iSCSI LUNs of 100 GB each will use only 55% of their capacity, you can create them all on a volume that can hold 5*100*.55=275 GB plus some room for growth (50 GB) = 325 GB.

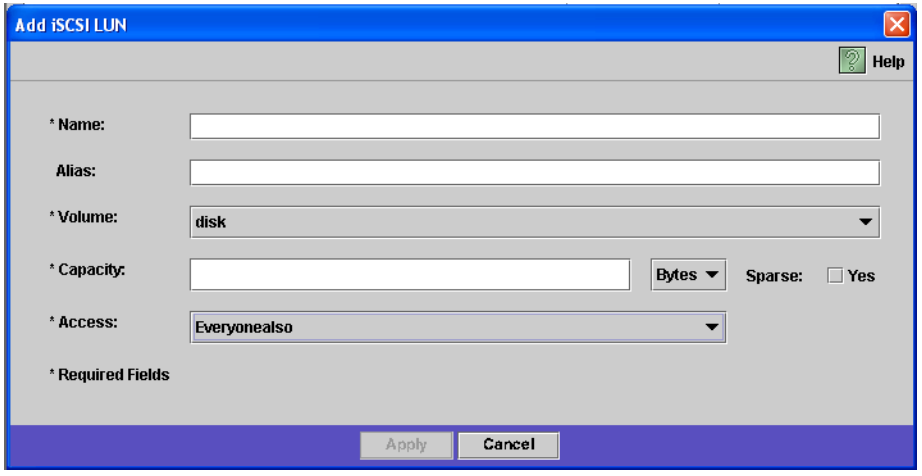
Using this model, you can monitor actual volume usage and allocate additional space to the volume before all the space is gone. If you expect that iSCSI LUN usage will use a majority of the available LUN size, you should not use the sparse LUN option. Some operating environments do not handle out of space conditions on sparse LUNs gracefully, so running out of actual space must be avoided to maintain optimal system behavior.

Creating an iSCSI LUN

To create an Internet Small Computer Systems Interface (iSCSI) logical unit number (LUN):

1. In the navigation pane, select iSCSI Configuration > Configure iSCSI LUN.
2. To add an iSCSI LUN to the list, click Add.

   The Add iSCSI LUN window is displayed.



3. Fill in the fields. For detailed information about the fields, click the Help button in the window, or see “Add/Edit iSCSI LUN Window” on page 336.
4. Click Apply to save the settings.

About iSCSI Target Discovery Methods

You can configure how an Internet Small Computer Systems Interface (iSCSI) initiator finds an iSCSI target by using one of the following methods:

- Static configuration – Manually add the iSCSI target name or Internet Protocol (IP) address to the iSCSI initiator host. Refer to the documentation provided with your iSCSI initiator software for details.
- SendTargets request – Add the iSCSI target portal IP address or Domain Name Service (DNS) name to the iSCSI initiator configuration. The initiator will issue a SendTargets request to discover the list of accessible iSCSI targets at the given target portal. Refer to the documentation provided with your iSCSI initiator software for details.
- Internet Storage Name Service (iSNS) server – Set up an iSNS server to automate the discovery of iSCSI initiators and iSCSI targets. An iSNS server enables iSCSI initiators to discover the existence, location, and configuration of iSCSI targets. The iSNS client is an optional feature and can be configured using the Web Administrator GUI as described in the next section.

Specifying an iSNS Server

To enable an Internet Storage Name Service (iSNS) server, you specify the Internet Protocol (IP) address or Domain Name Service (DNS) name of the iSNS server. The iSNS client interoperates with any standard iSNS server implementation, such as Microsoft iSNS Server 3.0.

To specify the iSNS server:

1. In the navigation panel, select iSCSI Configuration > Configure iSNS Server.
2. Type the IP address or DNS name of the iSNS server, and click Apply.

   You can also change the name of the iSNS server by entering a different IP address or DNS name in the iSNS Server field and clicking Apply.

Refer to your iSNS server documentation and iSCSI initiator documentation for more information.

Where to Go From Here

At this point, your file system and iSCSI targets are set up and ready to use. From here, you need to set up access privileges, quotas, and whatever directory structures you need. These management functions are described beginning in Chapter 4.

Monitoring functions, which are essential to managing resources, are covered in Chapter 10. Maintenance functions like backup and restore are covered in Chapter 11.

CHAPTER 4

System Management

This chapter describes several basic system management functions. These functions are primarily used only during initial system setup. However, they are available if you ever need to reset them.

This chapter includes the following sections:

Setting the Administrator Password

By default there is no password for the system administrator. You can set one if you so choose.

To set the system administrator password:

1. In the navigation panel, select System Operations > Set Administrator Password.
2. Enter the old password (if any) in the Old Password field.

   If there is no password, leave this field blank.
3. Enter the new password in the New Password field.

   The password must be at least 1 and no more than 20 characters long. There are no limitations on character type.

4. Enter the new password again in the Confirm Password field.

   If you want to disable passwords, leave the New Password and Confirm Password fields blank.

5. Click Apply to save your changes.

Controlling the Time and Date

This section provides information about controlling the time and date on the system. The following subsections are included:

About Controlling the Time and Date

Controlling the time and date on the system is essential for controlling file management. This section describes the functions available to maintain the correct time and date.

You can use time synchronization, or you can set the time manually.

Note: The first time you set the time and date you will also initialize the system's *secure clock*. This clock is used by the license management software and the Compliance Archiving Software to control time-sensitive operations.

Caution: Once the secure clock has been initialized, it cannot be reset. Therefore it is important that you set the time and date accurately when you are configuring the system.

About Time Synchronization

The system supports two types of time synchronization: Network Time Protocol (NTP) or RDATE Time Protocol. You can configure the system to synchronize its time with either NTP or an RDATE server.

- NTP is an Internet Protocol used to synchronize the clocks of computers to a reference time source, such as a radio, satellite receiver, or modem. Typical NTP configurations use multiple redundant servers and diverse network paths to achieve high accuracy and reliability.
- The RDATE time protocol provides a site-independent date and time. RDATE can retrieve the time from another machine on your network. RDATE servers are commonly present on UNIX systems, and enable you to synchronize system time with RDATE server time.

A third method, called "manual synchronization," disables time synchronization. In this method, the system administrator sets the system time and it tracks time independently from the other nodes on the network.

Setting Up Time Synchronization

You can set up either method of time synchronization in the Set Up Time Synchronization panel.

To set up time synchronization:

1. In the navigation panel, select System Operations > Set Up Time Synchronization.
2. Choose one of the following three options:
   - **Manual Synchronization** – Select this option if you do not want to use either NTP or RDATE time synchronization.
   - **NTP Synchronization** – Select this option if you want to use NTP synchronization and have at least one NTP server on the network.

     For detailed information about the NTP Synchronization options, see "Set Up Time Synchronization Panel" on page 376.
   - **RDATE Synchronization** – Select this option if you want to set up the RDATE server and tolerance window.

     For detailed information about the RDATE Synchronization options, see"Set Up Time Synchronization Panel" on page 376.
3. Click Apply to save your changes.

Setting the Time and Date Manually

If you do not use time synchronization, you can set the time and date manually.

To set the time and date manually:

1. In the navigation panel, select System Operations > Set Time and Date.
2. Select the correct year from the pull-down menu box above the calendar and to the left.
3. Select the correct month from the pull-down menu box above the calendar and to the right.
4. Click the correct date in the calendar.
5. Select the correct hour from the drop-down list box above the clock and to the left. The values range from 0 (midnight) to 23 (11:00 PM).
6. Select the correct minute (0 to 59) from the pull-down menu box above the clock and to the right.
7. Select the correct time zone from the pull-down menu at the bottom of the screen.

   Selecting the correct time zone enables the system to automatically adjust the setting for Daylight Saving Time.
8. Click Apply to save your time and date settings.

   Note: If this is the first time you have set the time and date on the system, this procedure will set the secure clock for managing complance files to the same time and date. Make sure that you set the time and date accurately, because you can only set the secure clock once.

Using Anti-Virus Software

This section provides information about using anti-virus software. The following subsections are included:

About Anti-Virus Software

Anti-virus protection is available through Internet Content Adaptation Protocol (ICAP) connections to "scan engines" that you have installed on your network. When you enable anti-virus protection on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, the system becomes a client of the anti-virus engine you are using on your network.

Note: If you configure virus protection on your system, you must have at least one scan engine operational at all times or Windows clients might be denied access.

About Virus Scanning

During normal operation, users of common internet file system (CIFS) clients might observe a short delay when virus scanning occurs, particularly with the Scan all Access option selected.

When a virus is detected, an entry is added to the system log that records the name of the infected file, the name of the virus, and what disposition was selected for the file. In most cases, the disposition is to "quarantine" the infected file and deny access to the CIFS client. Quarantined files are made visible in the `/quarantine` directory at the root of the file system containing the infected file. In order to avoid name conflicts in the `/quarantine` directory, files are named based on an "internal number:" *`NNNNNN`*`.vir` is a "hard link" to the infected file, and *`NNNNNN`*`.log` is a text file containing the original name of the infected file, and the details of the infections detected.

Note: By default, only the administrator (or UNIX root) can view the contents of the `/quarantine` directories.

The simplest way to recover from infected (quarantined) files is to delete them.

Enabling Anti-Virus Protection

To enable anti-virus protection:

1. In the navigation panel, select Anti Virus Configuration > Configure Anti Virus.

2. Select the Enable Anti Virus checkbox.

   Note: If you need to temporarily disable anti-virus scanning, use the Scanning Suspended option; do not clear the Enable Anti Virus checkbox.

3. Select the scan mode.

4. Specify the transmission control protocol/Internet Protocol (TCP/IP) address of the scan engine you want to use.

5. Specify the transmission control protocol/Internet Protocol (TCP/IP) port number on which the ICAP server listens for connections; this is typically port 1344.

6. Specify the maximum number of concurrent file scan operations that your system will dispatch to the scan engine; this is typically 2.

7. Specify what to include and exclude in each scan by selecting each from the displayed list.

8. To add a new item to a list, type it in the box and click Add.

   To remove an item from a list, select it and click Remove.

9. Click Apply to save your settings.

   Note: Files already in memory will not be subject to scanning. The best way to fully enable virus scanning is to reboot the system.

Deleting Quarantined Files

To delete quarantined files:

1. Determine the original name from either the system log or the *NNNNNN*`.log` file in the quarantine directory, and delete that file if it still exists.

2. Examine the quarantine directory for the two files *NNNNNN*`.vir` and *NNNNNN*`.log` corresponding to the infected file and delete those.

CHAPTER 5

System Port Management

This chapter describes network ports and alias IP addresses. You can bond two or more ports together to create a port bond. A port bond has higher bandwidth than the component ports assigned to it.

This chapter includes the following sections:

About Port Locations

The Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System identify ports in a predefined order based on their type and their physical and logical location on the server. To identify the port locations for your system, see the *Sun StorageTek 5320 NAS Appliance and Gateway Getting Started Guide*.

Each port must have an assigned role. The possible roles are as follows:

- **Primary** – The port role of Primary identifies an active network port. At least one port must be assigned a primary role. The Primary port is an integrated part of the failover process. When you assign this role to a port, the partner server (server H2) holds the Internet Protocol (IP) address assigned to the primary port as an offline, backup alias IP address. The reverse occurs when you supply an alias IP address on the partner server. The partner IP address is held as a backup alias IP address by the primary server (server H1). Should failover occur, the healthy server activates the partner server alias IP addresses, allowing network access to continue as if the failed server were still active.

  Note: At least one port on each server must be assigned a primary role.

- **Independent** – The port role of Independent identifies an active network port used for purposes other than serving data, such as backup. In a Sun StorageTek 5320 NAS Cluster Appliance the independent port does not participate in the failover process. Independent ports are typically used for remote backup. You cannot bond (aggregate) independent ports or add alias IP addresses to them. You can assign any number of independent port roles, but you should assign only one per head.
- **Mirror** – The port role of Mirror shows that the port connects this server to another server to mirror file volumes. Use the same port on both the source and target servers for mirroring. For more information about mirroring, see "About Sun StorageTek 5320 NAS Appliance Mirroring" on page 123.
- **Private** – (Sun StorageTek 5320 NAS Cluster Appliance only) The Private port is reserved for the heartbeat, a dedicated port that constantly monitors the status of the other head.

About Alias IP Addresses

Internet protocol (IP) aliasing is a networking feature that lets you assign multiple IP addresses to a single port. All of the IP aliases for the selected port must be on the same physical network and share the same *netmask* and *broadcast address* as the first, or primary, IP address specified for the selected port.

For single server (head) users only, you can add up to nine alias IP addresses to the primary IP address of each port. Therefore, a single network interface card (NIC) with two ports can provide up to 20 usable IP addresses.

On a Sun StorageTek 5320 NAS Cluster Appliance, IP aliasing is an integral part of the failover process. On a dual-head system, you can add up to four alias IP addresses to the primary IP address of each port. The five remaining IP alias positions are reserved for backing up primary and alias IP addresses of the primary and mirror ports on the partner server. In the event of head failover, the healthy server activates these reserved backup IP addresses, allowing network access to continue with minimal interruption. See "Enabling Head Failover" on page 20 for details on head failover.

For dual server systems, you can only add alias IP addresses to ports that are assigned a primary role. The role options are described in "About Port Locations" on page 67.

Note: Do not confuse the primary role with the primary IP address. The primary role is an assignment indicating how the port functions in a Sun StorageTek 5320 NAS Cluster Appliance. The primary IP address is the first address assigned to a selected port. In Web Administrator, the primary IP address is shown on the Network Configuration > Configure TCP/IP > Configure Network Adapters panel. You can select the port role at the bottom of the screen.

Bonding Ports

This section provides information about bonding ports. The following subsections are included:

About Port Bonding

There are two types of port bonding: port aggregation and high availability. Port aggregation bonding combines two or more adjacent ports to created a faster port, a port of greater bandwidth. High availability bonding combines two or more ports to provide network interface card (NIC) port failover services or backup ports.

Note: The Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System support Etherchannel bonding, a subset of the 802.3ad specification. Refer to your switch documentation for Etherchannel bonding before attempting to set up port bonding.

A system may have up to four bonds of any type. Each bond may have up to six ports.

About Port Aggregation Bonds

Port aggregation bonding (otherwise known as "channel bonding, aggregating, or trunking) lets you scale network I/O by joining adjacent ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth.

An aggregation bond requires a minimum of two available ports. The ports also must be of the same interface type (for example, Fast Ethernet with Fast Ethernet), connect to the same subnet, and must connect to adjacent ports on the same network switch.

Note: The switch attached to the ports configured for channel bonding must support IEEE 802.3ad link aggregation. Consult your LAN switch documentation for information about configuring this feature.

About High-Availability Bonds

High-availability (HA) port bonding provides port failover capabilities to the system. Two or more available ports are bonded so that if the primary port fails, a secondary port in the high-availability bond automatically takes over the burden to enable services to continue without any interruptions. As with port aggregation bonding, this type of bonding does not increase bandwidth.

In such a bond, at least two available ports are required. However, they do not have to be of the same type of interface card or connected to adjacent ports.

Note: Any type of switches can be used for an HA bond. The only requirement is that the switches must be connected to the same subnet.

Bonding Ports on a Single Server System

This section describes how to bond ports for a single server system.

You can bond ports after configuring them. However, alias Internet Protocol (IP) addresses and some other aspects of the original configurations might change. After you create a port bond, see "About Configuring Network Ports" on page 23 to configure the port bond. After you bond two or more ports, you cannot add IP aliases to the individual ports, only to the bond.

To bond ports on a single server system:

1. In the navigation panel, select Network Configuration > Bond NIC Ports.
2. Click Create.
3. Click either Port Aggregation or High Availability to designate the type of bond you want to create.
4. Choose at least two available ports to bond by clicking the desired port in the Available NIC Ports field, and then clicking > to add it to the NIC Ports in This Bond list.

If you chose Port Aggregation in Step 3, you must choose ports that have the same type of interface and are connected to adjacent ports.

To remove a port from this list, select the port and click <.

5. Type the required information in the IP Address, Subnet Mask, and Broadcast Address fields.

   By default these fields contain the information from the primary port, the first port listed in the NIC Ports in This Bond box.

6. Click Apply to complete the port bonding process. Web Administrator prompts you to confirm an automatic reboot.

   After the reboot, all alias IP addresses have been removed from the ports in the bond.

To add alias IP addresses to the port bond, see "Configuring Network Adapters" on page 23.

Bonding Ports on a Sun StorageTek 5320 NAS Cluster Appliance

To bond ports on dual server systems, you only need to complete the following procedure on one server. All ports in a port bond must be the same type (for example, Fast Ethernet with Fast Ethernet), connect to the same subnet, and connect to adjacent ports on the same network switch. The system automatically reboots immediately after each port bonding.

You can bond ports after configuring them. However, alias Internet Protocol (IP) addresses and some other aspects of the original configurations may change. After you create a port bond, see "About Configuring Network Ports" on page 23 to configure the port bond.

For more information on dual server port bonding, see "Example: Dual Server Port Bonding" on page 73.

Note: You can use only ports with a Primary role for port bonding. For more information about port roles, see "About Port Locations" on page 67.

To bond ports on a dual server system:

1. In the navigation panel, select Network Configuration > Bond NIC Ports.
2. Click Create.

3. Select the ports you want to bond from the Available NIC Ports list, which displays all ports that are not already part of a port bond.

   The window shows the IP Address, Subnet Mask, and Broadcast Address fields for the first port on the list.

4. Select a port, and then click > to add it to the NIC Ports in This Bond list.

   To remove a port from this list, select the port and click <.

   You must add at least two ports to the list. All ports in the bond must be on the same subnet.

   On the partner server, the corresponding ports are automatically bonded as well, after you click Apply and the server reboots. For example, if you bond Ports 2 and 3 on Server H1, Ports 2 and 3 on Server H2 are also bonded.

5. Click Apply to complete the port bonding process and reboot the system.

   The system automatically assigns a Bond ID to the new port bond. The IP address of the port bond is the same as the first port added to the bond.

6. To add alias IP addresses to the port bond, see "Configuring Network Adapters" on page 23.

   Once you bond two or more ports, you cannot add IP aliases to the individual ports, only to the bond.

Example: Dual Server Port Bonding

FIGURE 5-1 shows an example of a Sun StorageTek 5320 NAS Cluster Appliance connected to two different subnets. To show all possible combinations, this example represents each head as having a heartbeat port and four additional ports. All ports except the heartbeat port on each server are configured with a Primary role.

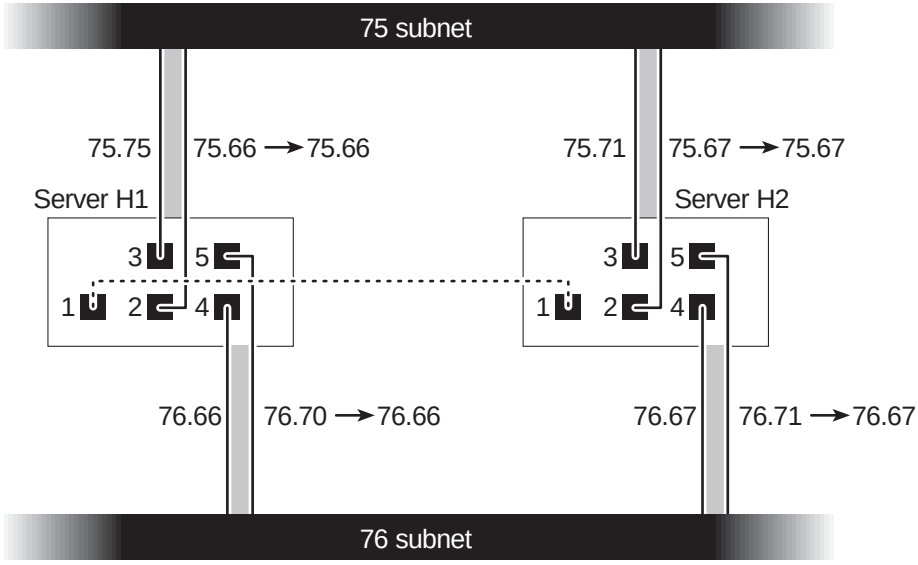


FIGURE 5-1 Dual Server Port Bonding

If Ports 2 and 3 are bonded, and Ports 4 and 5 are bonded, IP configuration is as listed in TABLE 5-1.

TABLE 5-1 Dual Server Port Bonding Example

	Ports to Be Bonded		Port Bond		
Head	Name	Primary IP Address	Name	Primary IP Address	Backup IP Address
	Port 2	192.1xx.75.66	Bond 1	192.1xx.75.66	192.1xx.75.67
	Port 3	192.1xx.75.70			
	Port 4	192.1xx.76.66	Bond 2	192.1xx.76.66	192.1xx.76.67
1	Port 5	192.1xx.76.70			

TABLE 5-1 Dual Server Port Bonding Example *(Continued)*

	Ports to Be Bonded		Port Bond		
Head	**Name**	**Primary IP Address**	**Name**	**Primary IP Address**	**Backup IP Address**
	Port 2	192.1xx.75.67	Bond 1	192.1xx.75.67	192.1xx.75.66
	Port 3	192.1xx.75.71			
	Port 4	192.1xx.76.67	Bond 2	192.1xx.76.67	192.1xx.76.66
2	Port 5	192.1xx.76.71			

The primary Internet Protocol (IP) address of each port on server H1 is the backup IP address for the corresponding port on server H2, and vice versa.

In the event of head failover, the surviving server activates the IP addresses of the failed server. You can add alias IP addresses to the primary IP address of a port bond and those IP addresses participate in the failover process. For more information about IP aliases, see "About Alias IP Addresses" on page 68.

CHAPTER 6

Active Directory Service and Authentication

This chapter describes Active Directory Service (ADS) in detail, Lightweight Data Access Protocol (LDAP) setup, and how to change name service lookup order. For setup instructions for other name services, refer to "Managing Name Services" on page 25.

This chapter includes the following sections:

About Supported Name Services

The Sun StorageTek system supports a variety of name services for both Windows networks and UNIX networks. These name services include:

- **ADS** – Active Directory Service (ADS) is a Windows 2000 name service integrated with the Domain Name Service (DNS, see "Setting Up DNS" on page 28). ADS runs only on domain controllers. In addition to storing and making data available, ADS protects network objects from unauthorized access and replicates objects across a network so that data is not lost if one domain controller fails. When you enable and set up ADS, the system automatically performs ADS updates. See "About Active Directory Service" on page 76 for more information.
- **LDAP** – Lightweight Data Access Protocol (LDAP) is a UNIX service that enables authentication.

- **WINS** – A Windows Internet Naming Service (WINS) server resolves NetBIOS names to Internet Protocol (IP) addresses, allowing computers on your network to locate other NetBIOS devices more quickly and efficiently. The WINS server performs a similar function for Windows environments as a DNS server does for UNIX environments. See "Setting Up WINS" on page 27 for more information.
- **DNS** – Domain Name Service (DNS) resolves domain names to IP addresses for the system. This service enables you to identify a server by either its IP address or its name. See "Setting Up DNS" on page 28 for more information.
- **NIS** – Network Information Service (NIS) configures the system to import the NIS database. It administers access to resources based on the users group and host information. See "Setting Up NIS" on page 29 for more information.
- **NIS+** – Network Information Service Plus (NIS+) was designed to replace NIS. NIS+ can provide limited support to NIS clients, but was mainly designed to address problems that NIS cannot address. Primarily, NIS+ adds credentials and secured access to the NIS functionality. See "Setting Up NIS+" on page 30 for more information.

Using Active Directory Service

This section provides information about the Active Directory Service (ADS) namespace and how to use it through the Web Administrator graphical user interface. The following subsections are included:

About Active Directory Service

Active Directory Service (ADS) is a Windows 2000 namespace that is integrated with the Domain Name Service (DNS). ADS runs only on domain controllers. In addition to storing and making data available, ADS protects network objects from unauthorized access and replicates objects across a network so that data is not lost if one domain controller fails.

For the Sun StorageTek system to integrate seamlessly into a Windows 2000 Active Directory Service environment, the following items must exist on the network:

- A Windows 2000 server domain controller
- An Active Directory–integrated DNS server that allows dynamic updates (needed in order to use the Dynamic DNS capability)

  Note: An Active Directory-integrated DNS server that allows dynamic updates is recommended but not required for using ADS.

Through the graphical user interface, you enable and configure ADS on the "Configure Domains and Workgroups Panel" on page 397. This enables the StorEdge software to automatically perform ADS updates.

After enabling and configuring ADS on the Configure Domains and Workgroups panel, you can enable ADS to publish StorEdge shares in the ADS directory. To do so, create or update SMB shares on the "Configure Shares Panel" on page 402 and specify the share container for each share that you want to publish.

Setting up ADS involves the following:

1. Enabling ADS, as described in "Enabling ADS" on page 77.
2. Verifying Name Service Lookup Order, as described in "Verifying Name Service Lookup Order" on page 79.
3. Verifying that DNS is enabled and configured to support ADS, as described in "Verifying DNS Configuration" on page 79.
4. Publishing shares in ADS, as described in "Publishing Shares in ADS" on page 80.

Enabling ADS

To enable Active Directory Service (ADS):

1. In the navigation panel, select System Operations > Set Time and Date.
2. Verify that the system time is within five minutes of any ADS Windows 2000 domain controller.
3. Click Apply to save any changes you make.

   Note: Resetting the date and time will change the system clock used for most time-related operations. It will not change the secure clock used by the license management software and the Compliance Archiving Software.
4. In the navigation panel, select Windows Configuration > Configure Domains and Workgroups.

5. Select the Enable ADS checkbox.
6. In Domain, enter the Windows 2000 Domain in which ADS is running.

   The system must belong to this domain.
7. In the User Name field, enter the user name of a Windows 2000 user with administrative rights.

   This user must be the domain administrator or a user who is a member of the domain administrators group. The ADS client verifies secure ADS updates with this user.

   Note: If you enter the domain administrator name here and the ADS update fails, the domain administrator password must be changed on the domain controller. This is only required for the administrator user, and the same password may be reused. For more information, refer to the Microsoft Support Services web site, Article Q248808.
8. In the Password field, enter the Windows 2000 administrative user's password.
9. In the Container field, enter the ADS path location of the Windows 2000 administrative user in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation.

   Objects, including users, are located within Active Directory domains according to a hierarchical path, which includes each level of "container" object. Enter the path in terms of the user's cn (common name) folder or ou (organizational unit).

   For example, if the user resides in a users folder within a parent folder called "accounting," you would type the following:

   `ou=users,ou=accounting`

   Do not include the domain name in the path.
10. If the ADS domain uses sites, enter the appropriate site name in the Site field. Otherwise, leave the Site field blank. If specified, the Site will be included when selecting a domain controller.
11. In the Kerberos Realm Info section, enter the Realm name used to identify ADS.
12. This is normally the ADS domain or the Domain Name Service (DNS) domain. When you click Apply, this entry is converted to all uppercase letters.
13. In the Server field, enter the host name of the of the Kerberos KDC server.

    The KDC server name is usually the host name of the main domain controller in the ADS domain. You can leave this field blank, if the system can locate the KDC server through DNS.
14. Click Apply to save and invoke your changes.

Verifying Name Service Lookup Order

To verify the name service lookup order:

1. Select UNIX Configuration > Configure Name Services.
2. Verify that the name service lookup order for Domain Name Service (DNS) is enabled by clicking the Hosts Order tab and ensuring that the DNS service is listed in Services Selected box.

   If it is not, select DNS service and click the > button.
3. (Optional) Set the name service lookup order to the correct priority by using the Up and Down buttons in the Services Selected box.

   This changes the order in which the selected services are scanned.
4. Click Apply to save any changes.

Verifying DNS Configuration

To verify Domain Name Service (DNS) configuration:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Set Up DNS.
2. If DNS is not enabled, select the Enable DNS checkbox.
3. If you have not entered a domain name, enter the DNS Domain Name.

   This name must be the same as the Active Directory Service (ADS) domain.
4. In the Server field, enter the Internet Protocol (IP) address of the DNS server you want the system to use, and then click the Add button to place the server address in the DNS Server List.

   You may add up to two servers to the list.
5. Select the Enable Dynamic DNS checkbox.

   If you do not enable Dynamic DNS, you must add the host name and IP address manually.

6. In the DynDNS User Name field, enter the user name of a Windows 2000 user with the administrative rights to perform secure dynamic DNS updates.

   You can leave this field blank for nonsecure updates if they are allowed by the DNS server.

7. In the DynDNS Password field, enter the password of the Dynamic DNS user.

8. Click Apply to save your changes.

   If Dynamic DNS is enabled, the system immediately updates DNS with its host name and IP address.

Publishing Shares in ADS

To publish shares in Active Directory Service (ADS):

1. In the navigation panel, select Windows Configuration > Configure Shares.

2. Click Add.

3. Enter a share name.

4. (Optional) Add a comment to describe the share.

   You can enter up to 60 alphanumeric characters.

5. Select a volume to share from the pull-down box.

6. (Optional) In the Directory field, enter an existing directory on the selected volume that you want to share.

   Note: A root-level share is created if the directory is omitted.

7. In the Container field, enter the location in the ADS directory where the share will be published.

   The Container field identifies the ADS container. Enter the ADS location for the share in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation. See step 9. on page 78 for more information.

8. Click Apply to add the share to the specified container.

   Note: The container specified must already exist for the share to be published in that container. The system does not create container objects in the ADS tree.

Updating ADS Share Containers

To update Active Directory Service (ADS) share containers:

1. In the navigation panel, select Windows Configuration > Configure Shares.
2. Select the share you want to update.
3. Click Edit to display the Edit Share window.
4. Enter the new share container.
5. Click Apply.

   The system updates the share container.

Removing Shares From ADS

To remove shares from Active Directory Service (ADS):

1. In the navigation panel, select Windows Configuration > Configure Shares.
2. Select the share you want to remove from ADS.
3. Click Edit to display the Edit Share window.
4. Delete the share container from the Container field.
5. Click Apply.

Setting Up LDAP

Before you can use Lightweight Data Access Protocol (LDAP), the LDAP server must be running.

To enable the LDAP service:

1. In the navigation panel, select UNIX Configuration> Set Up NSSLDAP.
2. To enable LDAP, check the Enable NSSLDAP checkbox.
3. In the Domain field, enter the domain name of the LDAP server, for example, `foo.com`.

4. In the Password field, enter the password set on the LDAP server.
5. In the Server field, enter the Internet Protocol (IP) address of the LDAP server.
6. In the Proxy field, enter the proxy domain, depending on the server settings.
7. Click Apply to save the settings.

Changing the Name Service Lookup Order

The name service (NS) lookup order controls the sequence in which the system searches the name services to resolve a query. These name services can include LDAP, NIS, NIS+, DNS, and Local. You must enable the services to use them for name resolution.

To set the order for user, group, Netgroup, and host lookup:

1. In the navigation panel, select UNIX Configuration > Configure Name Services.
2. Click on the Users Order tab to select the order of user lookup.
3. Select a service from the Services Not Selected box.
4. Click > to move it to the Services Selected box.

   To remove a service from user lookup, select it and click <.
5. Arrange the order of lookup services in the Services Selected box by selecting each service and clicking the Up or Down buttons to move it up or down.

   The service at the top of the list is used first in user lookup.
6. Click on the Groups Order tab to select the services to be used for group lookup, and perform steps 3-5.
7. Click on the Netgroup Order tab to select the services to be used for netgroup lookup, and perform steps 3-5.
8. Click on the Hosts Order tab to select the services to be used for hosts lookup, and perform steps 3-5.
9. Click Apply to save your changes.

CHAPTER 7

Group, Host, and File Directory Security

This chapter describes the various settings for local groups, hosts, user and group mapping, and file directory security. It includes the following sections:

Note: To configure Windows security, see "Configuring Windows Security" on page 26.

Managing Local Group Privileges

This section provides information about managing privileges for local groups. The following subsections are included:

About Local Groups

The requirements for Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System built-in local groups are different from those of a Windows system. With a network attached storage (NAS) appliance, there are no locally logged on users. All users attach through the network and are authenticated through a domain controller, so there is no need for local groups such as Users or Guests.

Note: Local groups apply only to common internet file system (CIFS) networking.

Local groups are primarily used to manage resources and to perform backup related operations. There are three local groups: administrators, power users, and backup operators.

- **Administrators** – Members of this group can fully administer files and directories on the system.
- **Power Users** – Members of this group can be assigned ownership of files and directories on the system, backup, and restore files.
- **Backup Operators** – Members of this group can bypass file security to backup and restore files.

The system also supports the Authenticated Users and Network built-in groups. All logged on users are automatically made members of both of these internally managed built-in groups. You can add any valid primary or trusted domain user as a member of any built-in local group.

About Configuring Privileges for Local Groups

Privileges provide a secure mechanism to assign task responsibility on a system-wide basis. Each privilege has a well-defined role assigned by the system administrator to a user or a group. On the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System, since there are no local users, privileges are only assigned to groups.

Unlike access rights, which are assigned as permissions on a per-object basis through security descriptors, privileges are independent of objects. Privileges bypass object-based access control lists to allow the holder to perform the role assigned. For example, members of the backup operators group must bypass the normal security checks to backup and restore files to which they would normally not have access.

The difference between an access right and a privilege is illustrated in the following definitions:

- An access right is explicitly granted or denied to a user or a group. Access rights are assigned as permissions in a discretionary access control list (DACL) on a per-object basis.
- A privilege is a system wide role that implicitly grants members of a group the ability to perform predefined operations. Privileges override or bypass object-level access rights.

The privileges supported are shown in TABLE 7-1.You can assign any of these privileges to any of the built-in groups. Because you can make any domain user a member of the built-in groups, you can assign these privileges to any domain user.

TABLE 7-1 Supported Privileges

Privilege	Description
Backup files and directories	Lets the user perform backups without requiring read access permission on the target files and folders.
Restore files and directories	Lets the user restore files without requiring write access permission on the target files and folders.
Take ownership of files and folders	Lets the user take ownership of an object without requiring take ownership access permission. Ownership can only be set to those values that the holder may legitimately assign to an object.

The default privileges assigned to the local built-in groups are shown in TABLE 7-2. Thus members of the local administrators group may take ownership of any file or folder and members of the Backup Operators can perform backup and restore operations.

TABLE 7-2 Default Group Privileges

Group	Default Privilege
Administrators	Take ownership
Backup operators	Backup and restore
Power users	None

About Ownership Assignment and Groups

By default, the Domain Admins group of the domain that the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System is a member of is a member of the local administrators group. Thus, when a member of the Domain Admins (including the domain administrator) creates or takes ownership of a file or folder, ownership is assigned to the local administrators group. This ensures maximum portability if the system is moved from one domain to another: objects owned by the local administrators group are still accessible to members of the new domain administrator group.

The ownership assignment rules described above are also true for regular users who are members of the local administrators group. If any member of the local administrators group creates or takes ownership of an object, ownership is assigned to the local administrators group rather than the member.

On Windows systems, the domain administrator membership of the local administrator group can be revoked. In such cases, members of the domain administrator group are treated as regular users. On the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System, however, the domain administrator is always assigned membership in the local administrators group. However, the domain administrator is not listed as a member of this group, so you cannot revoke its membership. Because there are no local users, and thus no local Windows administrators, the domain administrator group must have administrative control on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System.

Adding and Removing Group Members and Configuring Privileges

The Configure Groups panel lets you add any domain user to any of the three local groups.

To add a group, do the following:

1. In the navigation panel, select Windows Configuration > Configure Groups.
2. Click Add Group.

3. In the Group field, enter the name of the group.
4. In the Comment field, enter a description of or comments about the group.
5. Click Apply to save your changes.

To remove a group, do the following:

1. In the navigation panel, select Windows Configuration > Configure Groups.
2. Select the group you want to remove.
3. Click Remove Group.
4. Click Apply to save your changes.

To add or remove a group member, do the following:

1. In the navigation panel, select Windows Configuration > Configure Groups.
2. Highlight the group to which you want to add or from which you want to remove members.
3. Existing members for the selected group are listed in the Group Members box.
4. In the Group Members box highlight the member you want to add or delete, and click the Add or Delete icon.
5. Click Apply to save your changes.

To configure privileges for the group, use the Configure Privileges panel. For more information, see "Configuring NT Privileges for Groups" on page 87.

Configuring NT Privileges for Groups

To configure NT privileges:

1. In the navigation panel, select Windows Configuration > Configure Groups.
2. In the Groups box, select the group for which you want to assign privileges.
3. In the Group Privileges box, select the type of privileges that you want applied to the group.
4. Click Apply to save your changes.

Configuring Hosts

This section provides information about configuring hosts. The following subsections are included:

About Configuring Hosts

The Set Up Hosts panel enables you to add, edit, or remove entries from the system host file. The table shows current host information, including host name, host Internet Protocol (IP) address, and whether or not the host is trusted.

Caution: Exercise caution in granting trusted status to hosts. Trusted hosts have root access to the file system and have read and write access to all files and directories in that file system.

Adding and Editing Hosts

This section provides information about adding and editing hosts. The following subsections are included:

About Trusted Hosts

The Set Up Hosts panel lets you view and edit host information and designate whether a host is trusted. A `root` user on a network file system (NFS) client has root privileges on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System if that client was defined as a trusted host and has access to all files regardless of file permissions.

Manually Adding a Host

To manually add a host to the system configuration:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Set Up Hosts.
2. Click Add.
3. Enter the host name.

   This is the name by which the host is known on the system. The host name can include alphanumeric (a–z, A–Z, 0–9), "-" (dash) and "." (period) characters only. The first character must be alphabetical (a–z or A–Z only).
4. Type the Internet Protocol (IP) address of the new host.
5. If necessary, select the checkbox to assign the host Trusted status.

   A trusted host has root access to the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System.
6. Click Apply to save your changes.

Editing Host Information

To edit host information:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Set Up Hosts.
2. Select the host for which you want to edit information and click Edit.
3. Revise the host name, Internet Protocol (IP) address, and trusted status information as needed. For detailed information about these fields, see "Set Up Hosts Panel" on page 389.
4. Click Apply to save your changes.

Removing a Host Mapping for a Particular Host

To remove a host mapping for a particular host:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Set Up Hosts.

2. Select the host that you want to remove by clicking on the entry in the host list.
3. Click Remove.
4. Click Apply.

Adding and Editing Host Groups

This section provides information about adding and editing host groups. The following subsections are included:

About Adding and Editing Host Groups

The Set Up Hostgroups panel enables you to monitor and manage the host groups database. Groups and group members can be added to or deleted from this database. Host groups are used to define a collection of hosts that can be used for defining network file system (NFS) exports. Groups consist of predefined system groups and user-defined groups. The two predefined groups are the Trusted group and the iso8859 group.

Adding a Host Group

To add a host group:

1. In the navigation pane, select UNIX Configuration > Configure NFS > Set Up Hosts.
2. Click the Add icon () next to the Groups menu.

   The Add Hostgroup window is displayed.
3. Type the host group name.

   The host group name can include alphanumeric (a–z, A–Z, 0–9), "-" (dash) and "." (period) characters only. The first character must be alphabetical (a–z or A–Z only).
4. Click Apply to save your changes.

Adding a Member to a Host Group

To add a member to a host group:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Set Up Hosts.
2. Click the Add icon () next to the Group Members menu.

   The Add Hostgroup Member window is displayed.
3. Do one of the following:
   - **To add a host netgroup as a member,** select the Host Netgroup radio button and choose the Netgroup that you want from the drop-down menu.
   - **To add a host group as a member**, select the Host Group radio button and choose the host netgroup that you want from the drop-down menu.
   - **To add a host that you manually added on the Set Up Hosts panel or that exists on the NIS server as a member,** select the Known Host radio button and choose the host that you want from the drop-down menu.
   - **To add a host as a member that is not available from the Set Up Hosts panel**, select the Other Host radio button and type the name of the host in the field.
4. Click Apply to save your changes.

Mapping User and Group Credentials

This section provides information about mapping user and group credentials. The following subsections are included:

About Mapping User and Group Credentials

Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System servers are designed to reside in a multiprotocol environment and provide an integrated model for sharing data between Windows and UNIX systems. Although files may be accessed simultaneously from both Windows and UNIX systems, there is no industry-standard mechanism to define a user in both Windows and UNIX environments. Objects can be created using either environment, but the access control semantics in each environment are vastly different. This section addresses credential mapping. For details about the interaction between user or group credential mapping and the securable objects within the system, refer to "Mapping and Securable Objects" on page 244.

Credential mapping is used to establish an equivalence relationship between a UNIX user or group defined in a local configuration file or Network Information Service (NIS) database with a Windows domain user or group defined in an Windows Security Accounts Manager (SAM) database. User and group mapping is a mechanism to establish credential equivalence on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System to provide common access using either environment.

About UNIX Users and Groups

UNIX users and groups are defined in local configuration files (passwd and group) or in a Network Information Service (NIS) database. Each user and group is identified using a 32-bit identifier known, respectively, as a UID or a GID. Most UNIX systems use 16-bit identifiers but this has been extended to 32-bits on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System to avoid limitations imposed by the range of a 16-bit number. Although the UID or GID uniquely identifies a user or group within a single UNIX domain, there is no mechanism to provide uniqueness across domains. Traditionally, the value zero is applied to the root user or group. Root is granted almost unlimited access in order to perform administration tasks.

About Windows Users and Groups

Windows users and groups are defined in a Security Account Manager (SAM) database. Each user and group is identified by a security identifier (SID). A SID is a variable length structure that uniquely identifies a user or group both within the local domain and also across all possible Windows domains.

The format of a SID is as follows:

```
typedef struct _SID_IDENTIFIER_AUTHORITY {
       BYTE Value[6];
} SID_IDENTIFIER_AUTHORITY;
typedef struct _SID {
       BYTE Revision;
       BYTE SubAuthorityCount;
       SID_IDENTIFIER_AUTHORITY IdentifierAuthority;
       DWORD SubAuthority[ANYSIZE_ARRAY];
} SID;
```

The fields within the SID structure can be interpreted as shown in TABLE 7-3.

TABLE 7-3 Fields in the SID

Field	Value
Revision	The SID version. The current revision value is 1.
SubAuthorityCount	The number of subauthority entries in the SID. A SID can contain up to 15 subauthority entries.
IdentifierAuthority	A 6-byte array that identifies the subsystem that issued the SID.
SubAuthority	A 32-bit array of subauthorities uniquely identifies the appropriate security object: domain, user, group or alias. A domain SID uniquely identifies a domain amongst all other authority domains. A user, group, or alias SID is a domain SID with the appropriate relative identifier (RID) appended. A RID is a 32-bit identifier similar to a UNIX user identifier (UID) or group identifier (GID).

For readability, SIDs are often displayed as a string of the form: S-1–5-32-500. This SID contains a version number of 1, the identifier authority is 5 and it contains two subauthorities: 32 and 500. The value 500 is the RID.

Every Windows domain has a unique SID, and every Windows workstation and server designates a local domain named after its hostname. Thus every Windows workstation and server has a unique SID. Windows domains that span multiple machines are managed from a primary domain controller (PDC). The PDC provides centralized administration for the domain users and groups, and it defines a unique SID for the entire domain. Thus a domain user may be distinguished from a local workstation user by means of the domain part of the user SID.

To integrate with the Windows domain model, each Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System also generates a SID to define its local domain. The SID is generated using an algorithm that produces four subauthorities. The first subauthority has the value 4, which represents a nonunique authority. The other three subauthorities are generated using an algorithm that includes the current time and one of the system's MAC3 addresses to ensure uniqueness. This SID will be used to represent both local and Network Information Service (NIS) users by appending the UNIX UID or GID to the domain SID. This SID is stored in the equivalent of a local SAM database.

About Credential Mapping

User and group mappings can be defined to ensure that users can access their files from either Windows or UNIX systems. This section describes the algorithms used to automatically generate user and group mappings, and the policies applied during the login process. The mapping rules used to map UNIX users and groups to Windows users and groups are specified through system policy settings, and the specific mappings are held in the system policy database.

Each user mapping describes how a UNIX user with a specific user identifier (UID) is mapped to a Windows user in a specific domain with a specific relative identifier (RID). Similarly, each group mapping describes how a UNIX group with a specific GID is mapped to an Windows group in a specific domain with a specific RID.

The mapping format is as follows:

```
<UNIX-username>:<UID>:<Windows-username>:<NTDOMAIN>:<RID>
<UNIX-groupname>:<GID>:<Windows-groupname>:<NTDOMAIN>:<RID>
```

Local users and local groups are defined in the local `passwd` and `group` files. These files are defined using the following standard UNIX format:

```
<username>:<password>:<UID>:<GID>:<comment>:<home directory>:<shell>
<groupname>:<password>:<GID>:<comma-separated-list-of-usernames>
```

About User Mapping Policies

This section provides information about user mapping. The following subsections are included:

About User Mapping

User mapping is used to create an equivalence relationship between a UNIX user and an Windows user in which both sets of credentials are deemed to have equivalent rights on the system. Although the mapping mechanism supports full bi-directional mapping, there is no need to map UNIX users to Windows users for NFS access to the system. This is a result of a policy decision to use the UNIX domain as the base mapping domain.

Each time a Windows user logs in to the system, the mapping files are checked to determine the user's UNIX credentials. To determine the Windows user's UNIX user identifier (UID), the user map is searched for a match on the user's Windows domain name and Windows user name. If a match is found, the UNIX UID is taken from the matching entry. If there is no match, the user's UNIX UID is determined by the user mapping policy setting.

About User Mapping Policy Settings

There are four user mapping policy settings.

- **`MAP_NONE`** specifies that there is no predefined mapping between Windows users and UNIX users. A new unique UNIX user identifier (UID) will be assigned to the Windows user. The UID is tested for uniqueness by looking through the currently configured `passwd` database and the user map file and choosing a new UID. Typically the new UID will be one larger than the largest value found in the search. The passwd database may comprise the local network attached storage (NAS) `passwd` file and the Network Information Service (NIS) `passwd` file, if NIS is enabled. In this case, the mapping entry must be modified by hand if the Windows user should be mapped to an existing UNIX user.
- **`MAP_ID`** specifies that the UNIX UID is the Windows user's relative identifier (RID). No lookup is done on the `passwd` database.

- **MAP_USERNAME** specifies that the Windows user's user name is looked up in the `passwd` database. If a match is found between the Windows user name and the UNIX user name, the UNIX UID is taken from the matching entry. If no match is found, a unique UNIX UID is generated using the mechanism specified in `MAP_NONE` mechanism.
- **MAP_FULLNAME** specifies that the Windows user's Windows full name is looked up in the `passwd` database. A match is attempted with the UNIX comment field of each password entry. Only the full name entry of the comment field in the `passwd` database is compared with the Windows full name. If a match is found, the UNIX UID from the matching entry is used. If no match is found, a unique UNIX UID is generated as in the `MAP_NONE` mechanism.

The appropriate group credentials for the Windows user are obtained using the group mapping algorithm. For details, refer to "About Group Mapping" on page 96.

Example: User Mapping Policy

The following example shows a user map that makes the Windows user `HOMEBASE\johnm` equivalent to the UNIX user `john` and the Windows user `HOMEBASE\alanw` equivalent to the UNIX user `amw`.

```
john:638:johnm:HOMEBASE:1031
amw:735:alanw:HOMEBASE:1001
```

About Group Mapping Policies

This section provides information about group mapping. The following subsections are included:

About Group Mapping

Group mapping is used to create an equivalence relationship between a UNIX group and a Windows group. To determine the appropriate UNIX group identifier (GID) for a Windows user, the group map is searched using the user's Windows domain name and Windows primary group name. If a match is found, the map entry defines the UNIX GID to which the Windows user's group will be mapped. If there is no

matching entry in the group map, the UNIX GID is determined by the group map policy setting, and a new entry is created in the group map, with the exception of the `MAP_UNIXGID` policy.

About Group Mapping Policy Settings

There are four group mapping policy settings:

- **`MAP_NONE`** specifies that there is no predefined mapping between the Windows group and a UNIX group. A new unique UNIX group identifier (GID) will be assigned to the group. The GID is tested for uniqueness by looking through the currently configured `group` database and the `group` map file and choosing a GID that is one larger than the largest value found in the search. The `group` database may be comprised of the local network attached storage (NAS) `group` file and the Network Information Service (NIS) `group` file, if NIS is enabled. In this case the mapping entry must be modified by hand if the Windows group should be mapped to an existing UNIX group.
- **`MAP_ID`** specifies that the UNIX GID is the Windows user's group relative identifier (RID) as found in the user's access token.
- **`MAP_GROUPNAME`** specifies that the Windows user's group name is looked up in the `group` database. If a match is found, the UNIX GID is taken from the matching entry. If no match is found, a unique UNIX GID is generated.
- **`MAP_UNIXGID`** specifies that the Windows user's UNIX group is determined by the primary GID field in the `passwd` entry obtained during the user mapping operation.

  In this case, the `group.map` file is not consulted. If a GID cannot be determined, the UNIX nobody group GID (60001) is used.

The last step is to determine the list of UNIX groups to which the user belongs. The `group` database is searched for occurrences of the UNIX user name, as determined through the user mapping procedure. The GID of each group, in which the UNIX user name appears, is added to the group list in the user's credentials.

Example: Group Mapping Policy

The following example shows a group map that makes the `HOMEBASE\Domain Admin`s group equivalent to the UNIX `wheel` group and the `HOMEBASE\Domain Users` group equivalent to the UNIX `users` group.

```
wheel:800:Domain Admins:HOMEBASE:1005
users:100:Domain Users:HOMEBASE:513
```

The system default mapping rule will be `MAP_NONE` for both users and groups:

```
map.users=MAP_NONE
map.groups=MAP_NONE
```

There is no requirement for the user mapping rule to match the group mapping rule. An example of a possible mapping configuration is shown below. In this example, the user mapping rule is `MAP_USERNAME` and the group mapping rule is `MAP_ID`.

```
map.users=MAP_USERNAME
map.groups=MAP_ID
```

About Built-In Credential Mapping Policies

This section provides information about built-in credential mapping. The following subsections are included:

About Built-In Credential Mapping

The UNIX root identifier, 0 (user identifier (UID) or group identifier (GID)), is always mapped to the local Administrators group. The security identifier (SID) for the local Administrators group is a built-in (predefined) Windows SID: S-1-5-32-544. This mapping conforms to the ownership assigned by Windows to files created by the Domain Administrator. Ownership of such files is always assigned to the built-in local Administrators group to provide domain independence; that is, to avoid losing access to these files in the event that the system is moved from one Windows domain to another. In the Windows permissions display box this SID appears as `HOSTNAME\Administrators`, where `HOSTNAME` is the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System host name.

Defining the Mapping Policy

To define the mapping policy:

1. In the navigation panel, select Windows Configuration > Manage SMB/CIFS Mapping > Configure Mapping Policy.

2. Select a user mapping setting from the Windows <--> UNIX User Mapping Choice section. For detailed information about these settings, click the Help button in the panel, or see "Configure Mapping Policy Panel" on page 400.
3. Select a group mapping setting from the Windows <--> UNIX Group Mapping Choice section. For detailed information about these settings, click the Help button in the panel, or see "Configure Mapping Policy Panel" on page 400.
4. Click Apply to save your changes.

   For more detail about the interaction between user or group credential mapping and the securable objects within the system, see "Mapping and Securable Objects" on page 244.

Mapping Windows Groups and Users to UNIX Groups and Users

To map Windows groups and users to UNIX groups and users:

1. In the navigation panel, select Windows Configuration > Manage SMB/CIFS Mapping > Configure Maps.
2. Click Add.
3. In the NT User box, enter the following information:
   - **Account** – Enter the NT account name of the user or group you want to map.
   - **RID** – Enter the relative identifier that uniquely identifies the NT user or group within the NT domain.
4. In the UNIX User box, enter the following information:
   - **Name** – Enter the UNIX user or group name to which you want to map the specified NT user or group.
   - **ID** – Enter the identifier that uniquely identifies the UNIX user or group within the UNIX domain.
5. Click Apply to save your changes.

   For more information about the interaction between user or group credential mapping and the securable objects within the system, see "Mapping and Securable Objects" on page 244.

Editing a Mapping Between a Windows Group or User and a UNIX Group or User

To edit a mapping between a Windows group or user and a UNIX group or user:

1. In the navigation panel, select Windows Configuration > Manage SMB/CIFS Mapping > Configure Maps.
2. Select Users or Groups, depending on the type of mapping that you want to edit.
3. In the table, click the mapping that you want to edit, and click Edit.

   The Edit SMB/CIFS Group Map window is displayed.
4. In the NT User or the NT Group box, optionally edit the following information:
   - **Account** – Edit the NT account name of the user or group that is currently mapped.
   - **RID** – Edit the relative identifier that uniquely identifies the NT user or group within the NT domain.
5. In the Unix User or Unix Group box, optionally edit the following information:
   - **Name** – Edit the UNIX user or group name that is currently mapped to the specified NT user or group.
   - **ID** – Edit the identifier that uniquely identifies the UNIX user or group within the UNIX domain.
6. Click Apply to save your changes.

   For more information about the interaction between user or group credential mapping and the securable objects within the system, see "Mapping and Securable Objects" on page 244.

Setting File Directory Security

There are two methods for setting file directory security:

- "About Setting File Directory Security in Workgroup Mode" on page 101
- "Setting File Directory Security in Domain Mode" on page 101

About Setting File Directory Security in Workgroup Mode

In Workgroup/Secure Share mode, all security is set on the share itself (share-level security) using Web Administrator.

In Workgroup mode, the system assumes that no authentication is performed on the client and explicitly asks for permission requiring a password with every share-connection request.

See "Creating Static Shares" on page 106 for instructions on setting share-level security while adding a share. See "Editing an Existing SMB Share" on page 108 for instructions on setting share-level security while editing shares.

Setting File Directory Security in Domain Mode

You can manage access rights from Windows 2000 or Windows XP only.

Note: When the system is configured in Domain mode, the setting of object permissions is handled the same as object permissions on a standard Windows Domain controller. There is more than one right way to locate servers and map drives in order to set and manage share permissions. Only one example of this process is shown below.

Note: The Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System supports security on files and directories only, and setting security on a share will pass that security assignment to the underlying directory.

To set file directory security in Domain mode:

1. Open Windows Explorer.
2. Click Tools > Map Network Drive.
3. In the Map Network Drive window, select a drive letter from the Drive pull-down menu box.
4. Locate and select the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System.

5. Click OK.
6. From the Windows Explorer window, right-click on the system share for which you want to define user-level permissions.
7. Select Properties from the pull-down menu.
8. Select the Security tab in the Properties window.
9. Click the Permissions button.
10. Set the desired permissions.

    See your Windows documentation for more information on setting permissions.
11. Click OK.

CHAPTER 8

Shares, Quotas, and Exports

This chapter describes the various methods of controlling user access to the files and volumes on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System.

It includes the following sections:

Managing Shares

This section provides information about managing shares. The following subsections are included:

About Shares

Common Internet File System (CIFS) is an enhanced version of the Microsoft Server Message Block (SMB) Protocol. SMB/CIFS allows client systems of Windows environments to access files on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System.

A shared resource, or share, is a local resource on a server that is accessible to Windows clients on the network. On a Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, it is typically a file system volume or a directory tree within a volume. Each share is identified by a name on the network. To clients on the network, the share appears as a complete volume on the server, and they do not see the local directory path directly above the root of the share.

Note: Shares and directories are independent entities. Removing a share does not affect the underlying directory.

Shares are commonly used to provide network access to home directories on a network file server. Each user is assigned a home directory within a file volume.

There are two types of shares: static SMB/CIFS shares and autohome SMB/CIFS shares. Static shares are persistent shares that remain defined regardless of whether or not users are attached to the server. Autohome shares are temporary shares created when a user logs on to the system and removed when the user logs off.

When a user browses the system, only statically defined shares and autohome shares for connected users will be listed.

About Static Shares

A static share is created to allow users to map their home directories as network drives on a client workstation. For example, a volume `vol1` may contain a home directory named `home`, and subdirectories for users `bob` and `sally`. The shares are defined as shown in the following table.

TABLE 8-1 Share Path Examples

Share Name	Directory Path
`bob`	`/vol1/home/bob`

TABLE 8-1 Share Path Examples *(Continued)*

Share Name	Directory Path
sally	/vol1/home/sally

If defining and maintaining a static home directory share for each Windows user who has access to the system is inconvenient, you can use the autohome feature. See "About Autohome Shares" on page 110 for more information.

About Share Access Permissions

When you add a share by clicking Add on the Configure Shares panel, you have the option to specify Umask access permissions for the share. The Umask function is a three-digit number that is used to set access permissions for new directories and files in that share.

Of the Umask three-digit number, the first digit designates access permissions for the owner; the second number, the group; the third number, everybody. Each digit comprises of three bits designating read, write, and executable permissions. Bit 1 enables; bit 0 disables.

For example, enabling all three bits (111) grants read, write, and executable permissions. The octal equivalent value of "111" is "7" which you type in the Umask option box, accessible from the Configure Shares panel. Therefore, typing "777" in the Umask box grants all read, write, and executable permissions to the owner, the group, and everyone. Typing "700" grants read, write, and executable permissions only to the owner.

Note: If the DOS read-only attribute is set in a file create request, all write bits are disabled ("0") when the Umask option is applied. The following table illustrates this point.

TABLE 8-2 Umask Access Permissions With DOS Read-Only Attribute Set

Umask	New Directory Permissions		New File Permissions	
	DOS RW	DOS RO	DOS RW	DOS RO
000	777 (rwxrwxrwx)	777 (rwxrwxrwx)	666 (rw-rw-rw-)	444 (r--r--r--)
777	000 (---------)	000 (---------)	000 (---------)	000 (---------)
022	755 (rwxr-xr-x)	755 (rwxr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	775 (rwxrwxr-x)	664 (rw-rw-r--)	444 (r--r--r--)

Configuring Static Shares

This section provides information about configuring static shares. The following subsections are included:

About Configuring Static Shares

You use the Configure Shares panel to add, view, and update static Microsoft Server Message Block (SMB) shares.

The table at the top of the Configure Shares panel shows information about all existing SMB shares. This information includes the share name and directories shared, container names, and desktop database calls, as well as information concerning Windows Workgroups only (user, group, umask, and passwords).

Note: A volume or directory must exist before it can be shared.

By default, a hidden share is created for the root of each volume and is accessible only to Domain Administrators. These shares are typically used by administrators to migrate data and create directory structures. The share names can be found in the Configure Shares screen. The user shares are not created until after this step, as sharing directories at a point below the volume root eases security administration.

Creating Static Shares

You must create a file volume before you can create a share. For more information, see "About Creating a File Volume or a Segment" on page 46.

To add a new Microsoft Server Message Block (SMB) share:

1. In the navigation panel, select Windows Configuration > Configure Shares.
2. Click Add.
3. Type the name of the share you want to add in the Share Name field.
4. (Optional) Add a Comment to describe the share.

5. Select the Desktop DB Calls checkbox in the Mac Ext. section to allow the system to access and set Macintosh desktop database information.

6. Select the volume to share from the list of available volumes in the Volume Name pull-down menu.

7. Enter an existing directory in the Directory field.

   You cannot create a directory in this field. Directory names are case-sensitive.

   Note: Do not leave the Directory field blank.

8. (Optional) If you enabled ADS in the Set Up ADS panel, specify the ADS container in which to publish the share by typing the ADS path location for the share in the Container field. See "Publishing Shares in ADS" on page 80 for more information.

9. Enter the user ID, group ID, and password, if available.

   The User ID, Group ID, and Password fields are only available if you enable Windows Workgroup mode (not NT Domain mode). Refer to "Configuring Windows Security" on page 26 for information on enabling Windows security models.

   Windows Workgroup uses share-level security. The User ID (UID), Group ID (GID), and password fields in this screen represent the sole means of security for Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System file ownership and access by Windows Workgroup users. In other words, the rights to a directory are determined by the share definition rather than by the user. The system assumes that the client performs no authentication and explicitly asks for permission through the use of a password with every share-connection request.

   You can create multiple shares for the same directory with different UIDs, GIDs, and passwords. You can then give each user a password for a specific share. You can also manage individual user and group limitations on the amount of file volume space or number of files used through quotas. For more information about quotas, refer to "About Managing Quotas" on page 112.

   Caution: In the User ID field, enter the UID of the user accessing the specified directory through this share. The default value for this field is 0 (zero), which is the value of the UNIX root user. However, use caution in assigning this value. In Windows Workgroup mode, entering zero in this field disables all security on all files and directories in that share.

   - **R/W Password** – Enter the password for Windows Workgroup users who have read/write access to the directories specified for this share.
   - **Confirm R/W Password** – Re-enter the R/W password for confirmation.
   - **R/O Password** – Enter the password for Windows Workgroup users who have read-only access to the share.
   - **Confirm R/O Password** – Re-enter the R/O password for confirmation.

10. In the Umask field, enter the file creation mask, if any, you want to apply to this share.

    The umask defines the security policy for files and directories created in Share mode. It specifies the permission bits to turn off when a file is created.

    The umask is defined in octal because octal numbers are composed of three bytes, which maps easily to the UNIX file permission representation. The umask is applied using standard UNIX rules, except for the DOS read-only attribute. If the DOS read-only attribute is set when the file is created, all write bits will be removed from the file's permissions after the umask has been applied.

    The following table shows umask to permission examples, including the effect of the DOS read-only attribute. For more information, see "About Share Access Permissions" on page 105.

11. Click Apply to save your changes.

Editing an Existing SMB Share

To edit an existing Microsoft Server Message Block (SMB) share:

1. In the navigation panel, select Windows Configuration > Configure Shares.
2. Select the share you want to update.
3. Click Edit.
4. (Optional) If you want to change the old share name, type the new name in the Share Name field.
5. (Optional) Change the description of the share in the Comment field. You can enter up to 60 alphanumeric characters.
6. Select the Desktop DB Calls checkbox in the Mac Extensions section to let the system access and set Macintosh desktop database information.

    This speeds up Macintosh client file access and allows non-Macintosh clients to access Macintosh files on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System.

7. To change the share path, enter an existing directory name in the Path field.

    You cannot create a directory in this field. Directory names are case-sensitive.

8. Enter the new container, if necessary.

The container specifies the Active Directory Service (ADS) container in which the share is published. This field is available only if you have enabled ADS in the Set Up ADS panel. Enter the ADS path location for the share in LDAP DN notation. See "Enabling ADS" on page 77 for more information.

9. Enter the user ID, group ID, and password, if available.

   For detailed information about these fields, click the Help button on the panel, or see "Add/Edit Share Window" on page 393.

10. (Optional) Change the Umask setting using the rules specified for the Umask field. For more information, see "About Share Access Permissions" on page 105.

11. Click Apply to save your changes.

Removing an SMB/CIFS Share

To remove a Microsoft Server Message Block (SMB)/Common Internet File System (CIFS) share:

1. In the navigation panel, select Windows Configuration > Configure Shares.
2. Select the share you want to remove from the shares table.
3. Click Remove.
4. Click Apply to remove the share.

About Configuring SMB/CIFS Clients

After you have configured the security and network settings, the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System becomes visible to Microsoft Server Message Block (SMB)/Common Internet File System (CIFS) clients by automatically registering with the master browser on its local network.

Clients may connect in any of the following ways.

- **Windows 98, XP, and Windows NT 4.0**

Users connect either by mapping the network drive from Windows Explorer, or by clicking the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System icon in the Network Neighborhood window.

If they map the network drive, they need the Universal Naming Convention (UNC) path for the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, which consists of a computer name and share name as follows: `\\computer_name\share_name`. If they connect through Network Neighborhood, they need the system name used to identify the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System on the network.

- **Windows 2000, XP, and 2003**

If Active Directory Service (ADS) is not installed, users connect either by mapping the network drive from Windows Explorer, or by clicking the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System icon in the My Network Places window.

If they map the network drive, they need the UNC path for the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, which consists of a computer name and share name as follows:
`\\computer_name\share_name`. If they connect through Network Neighborhood, they need the system name used to identify the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System on the network.

If ADS is installed, users can connect by clicking on a Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System share published in ADS.

- **DOS**

Users must type the `net use` command to map a share to a drive letter on the command line. They need the UNC path for the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System, which consists of a computer name and share name as follows: `\\computer_name\share_name`.

About Autohome Shares

The Microsoft Server Message Block (SMB)/Common Internet File System (CIFS) autohome share feature eliminates the administrative task of defining and maintaining home directory shares for each Windows user accessing the system. The system creates autohome shares when a user logs on and removes them when the user logs off. This reduces the administrative effort needed to maintain user accounts and increases the efficiency of server resources.

To configure the autohome feature, enable it and provide an autohome path. The autohome path is the base directory path for the directory shares. For example, if a user's home directory is `/vol1/home/sally`, the autohome path is `/vol1/home`. The temporary share is named `sally`. The user's home directory name must be the same as the user's logon name.

When a user logs on, the server checks for a subdirectory that matches the user's name. If it finds a match and that share does not already exist, it adds a temporary share. When the user logs off, the server removes the share.

Windows clients might automatically log a user off after 15 minutes of inactivity, which results in the autohome share disappearing from the list of published shares. This is normal CIFS Protocol behavior. If the user clicks on the server name or otherwise attempts to access the system (for example, in an Explorer window), the share automatically reappears.

Note: All autohome shares are removed when the system reboots.

Because autohome shares are created and removed automatically, configuring them is largely a matter of enabling the feature.

Enabling Autohome Shares

Note: When configuring a user's home directory using the Active Directory administrative tool, you will get a warning indicating the autohome path cannot be found. You can ignore this message because the autohome share will be created when the user logs on.

To enable autohome shares:

1. In the navigation panel, select Windows Configuration > Configure Autohome.
2. Select the Enable Autohome checkbox.
3. Enter the autohome path.

   For more information on the path, see "About Autohome Shares" on page 110.
4. Enter the ADS Container.

   For more information, see "About Active Directory Service" on page 76.
5. Click Apply to save your changes.

Managing Quotas

This section provides information about managing quotas. The following subsections are included:

About Managing Quotas

The Manage Quotas panel enables you to administer quotas on Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System file volumes and directories. User and group quotas determine how much disk space is available to a user or group and how many files a user or group can write to a volume. Directory tree quotas determine how much space is available for a specific directory and/or how many files can be written to it.

See "About Configuring User and Group Quotas" on page 113 to set space and file limits for users and groups. Refer to "About Configuring Directory Tree Quotas" on page 115 to set space and file limits for specific directories.

Configuring User and Group Quotas

This section provides information about configuring user and group quotas. The following subsections are included:

About Configuring User and Group Quotas

The Configure User and Group Quotas panel lets you administer quotas on volumes for NT and UNIX users and groups. It displays root, default, and individual quotas for the volume selected. The settings for the default user and default group are the settings used for all users and groups that do not have individual quotas.

A hard limit is the absolute maximum amount of space available to the user or group.

Reaching a soft limit, which is equal to or lower than the hard limit, triggers a grace period of seven days. After this grace period is over, 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 are automatically set to have no hard or soft limits for space or files and cannot have quotas defined.

Enabling Quotas for a File Volume

To enable quotas for a file volume:

1. In the navigation panel, select File Volume Operations > Edit Volume Properties.
2. Select the file volume for which you are enabling quotas from the Volume Name pull-down menu.
3. Be sure there is a check mark in the Enable Quotas box. If not, select the box.
4. Click Apply.

Adding a User or Group Quota

To add a user or group quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure User and Group Quotas.
2. Click Users if you are configuring a user quota, or Groups if you are configuring a group quota.

3. Select the name of the file volume for which you are adding a quota from the drop-down Volume list.

   The table on this screen shows the root, default, and individual user or group quotas for the file volume selected.

4. To add a quota for a user or group, click Add.

5. Select whether the designated user or group belongs to a UNIX or NT environment by clicking on the appropriate option button.

6. Select the appropriate user or group name (and Domain name for NT users or groups).

7. Set the disk space limits for the selected user or group. For detailed information on the disk space limits, click the Help button in the window, or see "Add/Edit Quota Setting Window" on page 319.

8. Set limits on the number of files a user or group can write to the file volume. For detailed information on the file limits, click the Help button in the window, or see "Add/Edit Quota Setting Window" on page 319.

9. Click Apply to save your changes.

Editing a User or Group Quota

To edit a user or group quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure User and Group Quotas.

2. Click Users to edit a user quota or Groups to edit a group quota.

3. Select the name of the file volume for which you are editing quotas from the drop-down Volume list.

   The table on this screen shows the root, default, and individual user or group quotas for the file volume.

4. Select the user or group for whom you are editing a quota, and click Edit.

5. Edit the disk space limits for the selected user or group. For detailed information on the disk space limits, click the Help button in the window, or see "Add/Edit Quota Setting Window" on page 319.

6. Edit the limits on the number of files a user or group can write to the file volume. For detailed information on the file limits, click the Help button in the window, or see "Add/Edit Quota Setting Window" on page 319.

7. Click Apply to save your changes.

Deleting a User or Group Quota

Root and default quotas cannot be deleted. You can remove an individual quota by setting it to disk space and file defaults.

To delete a user or group quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure User and Group Quotas.
2. In the Configure User and Group Quotas panel, select Users to remove a user quota or Groups to remove a group quota.
3. Select the quota you want to remove in the table and click Edit.
4. In the Edit Quota Setting window, click the Default option in both the Disk Space Limits and File Limits sections.
5. Click Apply to remove the quota setting.

Configuring Directory Tree Quotas

This section provides information about configuring directory tree quotas. The following subsections are included:

About Configuring Directory Tree Quotas

The Configure Directory Tree Quotas (DTQ) panel lets you administer quotas for specific directories in the file system. Directory tree quotas determine how much disk space is available for a directory and how many files can be written to it. You can only configure quotas for directories created in this panel, not for previously existing directories.

Creating a Directory Tree With a Directory Tree Quota

To create a directory tree with a directory tree quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure Directory Tree Quotas.
2. Select the file volume for which you are configuring a directory tree quota from the pull-down menu.
3. Click Add.
4. In the DTQ Name field, enter a name to identify this directory tree quota.
5. In the DirName field, enter a name for the new directory.
6. Underneath the Path field, there is a box that shows the directory tree structure for the file volume you selected.

   To view the contents of a folder, click the symbol next to the folder or double-click the folder icon. Then select the directory that will contain the new directory that you are creating. Continue until the full path of the directory is shown in the Path field.
7. Select the disk space limit for the directory in the Disk Space Limits section, selecting either No Limit or Custom.
   - Select No Limit to allow unlimited disk space for the directory.
   - Select Custom to define the maximum disk space that the directory can occupy.
8. Choose whether the quota is reported in megabyte or gigabyte and enter the disk space limit in the Max Value field.

   Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.
9. In the File Limits field, select the maximum number of files that can be written to this directory, either No Limit or Custom.
   - Select No Limit to allow an unlimited number of files to be written to this directory.
   - Select Custom to assign a maximum number of files. Then enter the file limit in the Max Value field.
10. Click Apply to add the quota.

Editing an Existing Directory Tree Quota

To edit an existing directory tree quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure Directory Tree Quotas.
2. Select the quota you want to edit from the table, then click Edit.
3. Edit the name that identifies this directory tree quota in the DTQ Name field.

   The Path is a read-only field that shows the path of the directory.
4. In the Disk Space Limits section, select the disk space limit for the directory, selecting either No Limit or Custom.
   - Select No Limit to allow unlimited disk space usage for the directory.
   - Select Custom to assign a maximum amount of disk space.
5. Choose whether the quota is reported in megabyte or gigabyte, and enter the disk space limit in the Max Value field.

   Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.
6. In the File Limits section, select the maximum number of files to be written to this directory, selecting either No Limit or Custom.
   - Select No Limit to enable you to write an unlimited number of files to this directory.
   - Select Custom to assign a maximum number of files.
7. Enter the file limit in the Max Value field.
8. Click Apply to save your changes.

   Note: When you move or rename a directory that contains a directory tree quota (DTQ) setting, the system automatically updates the DTQ's path specification.

Deleting a Directory Tree Quota

To delete a directory tree quota:

1. In the navigation panel, select File Volume Operations > Manage Quotas > Configure Directory Tree Quotas.
2. Select the quota you want to remove from the table.
3. Click Delete to remove the quota setting.

   Deleting a directory tree quota (DTQ) removes the quota setting. However, it does not delete the directory itself or the files in the directory.

Note: If you delete a directory that contains a DTQ setting, both the directory and the DTQ setting are deleted.

Setting UP NFS Exports

This section provides information about setting up NFS exports. The following subsections are included:

About Setting Up NFS Exports

Network File System (NFS) exports let you specify access privileges for UNIX (and Linux) users. The table in the Configuring Exports panel shows the current NFS export information, including the accessible directories, host name, and access level (Read/Write or Read/Only) for each export.

Any host name beginning with "@" identifies a group of hosts. For example, a host name of `@general` includes all hosts, and a host name of `@trusted` includes all trusted hosts. Refer to "About Configuring Hosts" on page 88 for information about trusted hosts.

You create exports by specifying access privileges for a particular UNIX host.

Creating Exports

To create an export:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Configure Exports.

   The table in this panel shows the current export information. If you have not created any exports, this space is blank.

2. Click the Add button to add an export.

3. In the Volume box, select the volume for which you want to grant UNIX NFS host access.
4. In the Path box, specify the directory for which you want to grant UNIX NFS host access.

   Leaving this field blank exports the root directory of the volume.
5. In the Access section, specify whether the hosts have Read/Write, Read/Only, or No Access privileges on the selected volume.
6. In the Hosts section, select the host or hosts for which you are defining a Network File System (NFS) export.

   Choose from the following:

   - **Host Netgroups** – To select a netgroup, select this option button. From the drop-down menu, select the netgroup for which you are defining this export.
   - **Host Group** – To select a host group, select this option button. From the pull-down menu, select either general (all hosts), trusted (all trusted hosts), or a user-defined host group.
   - **Known Host** – To assign the export to a host added through the Set Up Hosts panel, select this option. From the pull-down menu, select the host for which you are defining this export.
   - **Other Host** – To assign the export to an individual host that you have not added through the Set Up Hosts panel, select this option and type in the name of the host.
7. In the Map Root User section, select a method for mapping the user ID for root users.

   Choose from the following:

   - **Anonymous users** – To map the user ID of root users to the user ID of anonymous users, select this option button.
   - **Root User** – To map the user ID of root users to the user ID of root (UID=0), select this option button.
   - **Map to UID** – To assign a specific user ID, select this option and enter the user ID.
8. Click Apply to save the export.
9. In the Configure Exports panel, verify that the correct path, host, and access rights are shown for the export you created.

Editing Exports

To edit an export:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Configure Exports.
2. Select the export you want to change, and click the Edit button.
3. To change the Access rights, click Read/Write, Read/Only, or No Access.

   The Hosts section is read-only.
4. Click Apply to save your changes.
5. In the Configure Exports panel, verify that the correct path, host, and access rights are shown for the export you edited.

Removing Exports

To remove a Network File System (NFS) export:

1. In the navigation panel, select UNIX Configuration > Configure NFS > Configure Exports.
2. Click the Trash button.
3. Confirm the removal.

CHAPTER 9

System Options

This chapter provides instructions for activating options you can purchase for the Sun StorageTek 5320 NAS Appliance systems. Additionally, details about the following options are included in this chapter:

- Sun StorageTek File Replicator Software, which allows you to duplicate data from one volume onto a mirrored volume on a different Sun StorageTek 5320 NAS Appliance (typically used for transaction-oriented systems)
- Sun StorageTek Compliance Archiving Software, which allows you to enable volumes to follow compliance archiving guidelines for data retention and protection

This chapter includes the following sections:

Activating System Options

To activate system options, you must enter an activation key in the Activate Options panel. If you have purchased an option, contact your Sun Microsystems customer service representative for the activation key.

To activate a system option:

1. In the navigation panel, select System Operations > Activate Options and click Add to add the license.
2. In the Add License window, type the module name provided by Sun (for example, `Sun StorageTek File Replicator`).
3. Enter the origination date provided by Sun, in the format *YYYYMMDD*.

This is the date on which the license becomes active, starting at 0000:00 hours. The date 00000000 means the license is active immediately.

4. Enter the expiration date provided by Sun, in the format *YYYYMMDD*.

   This is the date on which the license expires at 2359:59 hours. The date 00000000 means the license does not expire.

   Note: When a compliance license expires or is removed, the system will maintain compliance rules, but no new compliance volumes can be created. Refer to "About Compliance Archiving Software" on page 136 for more information about the Compliance Archiving Software.

5. Enter the license key provided by Sun.

6. Click Apply to activate the option.

   For the Sun StorageTek File Replicator Software software, you must perform additional steps on the mirrored server. Refer to "Activating Sun StorageTek File Replicator Software Software on the Remote Server" on page 127 for instructions.

7. If you have never set the time and date, enter the correct time, date, and time zone information.

   This will set the system time and the secure clock. The license manager software and the Compliance Archiving Software use the secure clock for sensitive time-based operations.

   Note: The secure clock can only be set once. Make sure you set it accurately.

8. Confirm that the new time and date are accurate.

   If the new time and date are correct, click Yes. If not, click No and set the time and date correctly.

About the Sun StorageTek File Replicator Software Option

This section provides information about the Sun StorageTek File Replicator Software option. The following subsections are included:

About Sun StorageTek 5320 NAS Appliance Mirroring

Mirroring enables you to duplicate any or all of the file volumes of one Sun StorageTek NAS system onto another Sun StorageTek NAS system. The source server is called the "active server" and the target server is called the "mirror server."

In the event that the active server fails, you can break the mirror on the mirror server, and then promote the mirrored file volume (make it available for users) on the mirror server.

The mirroring method used is an asynchronous transaction-oriented mirror. Mirroring is accomplished through a large mirror buffer to queue file system transactions for transfer to the mirror system. In practice, the mirror server lags the active server by a short time period. Because the mirror is transaction-oriented, the integrity of the mirror file system is guaranteed, even during network interruptions or system outages.

About Preparing for Mirroring

Before you begin mirroring, make sure you have the following:

- Two Sun StorageTek NAS servers are required for mirroring. The servers may be of any model and can be of differing models.
- The mirror server must contain an equal or larger amount of storage space than the file volumes to be mirrored.
- There must be a reliable, continuously available network connection with sufficient capacity between the active and mirror servers. The interface type connecting these two servers can be 100 megabit Ethernet or 1000 megabit Ethernet. The servers may be connected through a switch or router. If you are connecting the servers to a router, be sure to configure the static route setting to

ensure that the mirroring data is directed through the private route. If you are connecting the servers to a switch, create a virtual LAN (VLAN) for each server to isolate network traffic.

- Both servers must have the same version of the operating system installed.
- The active file volumes to be mirrored must be at least 1 gigabyte.

  Note: Once a file volume is mirrored, the original file volume cannot be renamed.

About Requirements and Limitations For Cluster Configurations

The following is a list of requirements and limitations for mirroring with Sun StorageTek File Replicator Software software in a Sun StorageTek 5320 NAS Cluster Appliance configuration:

- Both servers in the cluster configuration should have the Sun StorageTek File Replicator Software license enabled.
- Mirrors should be established only from and to server H1. (Do not create a mirror from server H1 to server H2 of the same cluster.)
- To perform any mirror management operations (including New Mirror creation, Change Role, Promote, and Break), both servers in the cluster should be in the NORMAL state.
- When the cluster is in failover mode (that is, one server is in the ALONE state and the other server is in the QUIET state) or any degraded state, *do not* perform any mirror management operations. You should bring the cluster to the NORMAL state before doing any of the mirror management operations.
- Existing mirrors will continue mirroring, even when the cluster configuration fails over. Also, the existing mirrors will continue mirroring when the cluster is restored after a failover.
- Mirror buffering restrictions as described in "About Mirroring the Mirror Buffer" on page 126,

Configuring Active and Mirror Systems

When setting up your systems, designate the roles of the ports connecting the mirroring servers to one another. Then configure mirroring on the active and mirror systems using the Web Administrator interface (see "About Mirroring the Mirror Buffer" on page 126). Configure each system independently.

To configure the dedicated network ports:

1. In the navigation panel of the active server, select Network Configuration > Configure TCP/IP > Configure Network Adapters.
2. If you have not done so already, assign the Internet Protocol (IP) addresses and a port role of Primary for the ports that are connected to a local network or subnet.

   The active and mirror systems' ports can be on different local subnets. For more information about configuring transmission control protocol/Internet Protocol (TCP/IP), see "About Configuring Network Ports" on page 23.
3. Assign the IP address for the port used for the mirroring connection between the active and mirror systems.

   Note: Do not use the subnet containing the primary interface for mirroring.

   If you have created an isolated network to carry the mirroring traffic, you should use addresses in the range reserved for private use, such as `192.1xx.x.x`. For example, assign the active system's mirror link interface to `192.1xx.1.1`, and assign the mirror system's mirror link interface to `192.1xx.1.2`.
4. In the Role field of the port used for the connection between the active and mirror servers, select Mirror.
5. If the mirror interfaces of the active and mirror systems are not connected on the same subnet, you must set up a static route between them using the command-line interface.

   This enables the servers to communicate with each other over networks that are not directly connected to their local interfaces. For more information about completing this process, see "Managing Routes" on page 226.
6. Click Apply to save changes.

Configuring Mirrored File Volumes

This section provides information about configuring mirrored file volumes. The following subsections are included:

About Mirroring the Mirror Buffer

Mirroring is performed on a per-volume basis. You may choose to mirror some or all of your volumes.

Note: Only file volumes equal to or larger than 1 gigabyte can be mirrored. Once a file volume is mirrored, the original file volume cannot be renamed while the mirroring connection is maintained.

There can be no I/O activity to the file volume being mirrored from the active server during initial mirror synchronization.

The mirror buffer stores file system write transactions while they are being transferred to the mirror server. The file volume free space on the active server is reduced by the allocation size of the mirror buffer.

The size of the mirror buffer depends on a variety of factors, but must be at least 100 megabytes, and the mirror buffer can never be more than half of the remaining free space on any given file volume.

In a normal scenario, you should create a mirror buffer that is approximately 10 percent of the size of the file volume you are mirroring. The size you choose should depend on how much information is being written to the file volume rather than the size of the file volume. As a rule of thumb, the size of mirror buffer is directly proportional to the frequency of writes to the file volume and inversely proportional to the speed of the network connection between the two servers.

If there is high write activity to the file volume and a slow network connection between the two mirror servers, you should create a mirror buffer that is approximately 25 to 30 percent of the size of the file volume you are mirroring.

The size of the mirror buffer cannot be dynamically increased. To increase the size of the mirror buffer, you have to break the existing mirror and create the mirror again with the new mirror buffer size.

Activating Sun StorageTek File Replicator Software Software on the Remote Server

After you have activated the Sun StorageTek File Replicator Software option (see "Activating System Options" on page 121), you must also activate the option on the remote server that contains file volumes you want to mirror.

To activate Sun StorageTek File Replicator Software option on the remote server:

1. Log in to Web Administrator on the server containing the file volumes you want to mirror.
2. In the Add License window type the module name provided by Sun (`Sun StorageTek File Replicator Software`).
3. Enter the Origination date provided by Sun in the format *YYYYMMDD*.

   This is the date on which the license becomes active starting at 0000:00 hours. The date 00000000 means the license is active immediately.
4. Enter the Expiration date provided by Sun in the format *YYYYMMDD*.

   This is the date on which the license expires at 2359:59 hours. The date 00000000 means the license does not expire.
5. Enter the license key provided by Sun.
6. Click Apply to activate the Sun StorageTek File Replicator Software software.

Adding a File Volume

To add a file volume to the configuration:

1. In the navigation panel, select File Replicator > Manage Mirrors.
2. Click Add.
3. Select the file volume to be mirrored from the Volume pull-down menu.

   The file volume to be mirrored must be equal to or larger than 1 gigabyte.
4. Type a distinct name for the mirror server in the Mirror Host field.

5. Type the Internet Protocol (IP) address of the mirror system.

   This must be the IP address chosen for the mirroring network interface card (NIC) on the mirror system.

6. (Optional) Type the alternate IP address.

   In the event that the first IP address becomes unavailable, the server uses the alternate IP address to maintain the mirror.

7. If an administrative password is required to access the mirror server, enter it in the Password field.

   If there is no administrative password, leave this field blank. Always protect your servers with passwords.

8. Enter the size (in megabytes) of the mirror buffer.

   The file volume free space on the active server is reduced by the allocation size of the mirror buffer.

9. Make sure there is no I/O activity to the source file volume on the active server while the mirror is being created, and then click Apply to create the mirror.

   The mirror creation process begins. When the mirror reaches an In Sync status in the Manage Mirrors panel, the mirrored file volume is mounted as read-only. I/O activity can resume once the mirror reaches In Sync status.

   You can edit the alternate IP address or mirror server administrator password of an existing mirror.

Editing a Mirror

To edit a mirror:

1. In the navigation panel, select File Replicator > Manage Mirrors.
2. Select the mirror that you want to edit from the table.
3. Click Edit.

   The file volume name and mirror host are read-only fields.

4. Edit the Internet Protocol (IP) address you want to use for the mirror connection, and then edit the alternate IP address in the next field.
5. If necessary, enter the new administrator password required for accessing the mirror host server.

   If there is no administrative password, leave the Password field blank.

6. Click Apply to save your changes.

Correcting a Cracked Mirror

In the event a mirror cracks (this happens if the connection between the two servers is down for some time or if the mirror buffer is too small and there are many writes to the master volume), you can correct the cracked mirror.

To correct a cracked mirror:

1. Establish a faster network connection between the two servers.
2. Quiesce all the I/O activity to the master file system, until the mirror reaches the In Sync state.
3. After you break and promote the `nbd` volume, mount the target file system on the mirror server as read-only from either the Common Internet File System (CIFS) or Network File System (NFS) client.

   This file system can be used for backup or any read-only activity.

   You can also combine checkpoints with the mirroring functionality. When a checkpoint is created on the active server, the checkpoint also gets mirrored to the mirrored server. This can be used for scheduled backups or to give read-only checkpoint access to other users and applications.

Setting Warning Thresholds for Mirrored File Volumes

This section provides information about setting warning thresholds. The following subsections are included:

About Setting Warning Thresholds

In the File Replicator > Set Threshold Alert panel you can set the threshold alert for all mirrored file volumes. The threshold alert is the percentage of mirror buffer use at which a warning is sent to designated recipients.

The mirror buffer stores file system write transactions while they are being transferred to the mirror server. Increases in write activity to the active server or a damaged network link can cause the transference of write transactions to the mirror server to "back up" in the mirror buffer. If the mirror buffer overruns because of this process, the mirror is cracked and no further transactions occur between the active server and the mirror server until the mirror is reestablished. Once full communication is restored, the system automatically begins the mirror resync process until the mirrored file volume is back in sync.

To prevent this situation, the system automatically sends warnings through email notification, the system log file, Simple Network Management Protocol (SNMP) traps, and the LCD panel when the mirror buffer is filled to certain threshold percentages.

Setting Up the Threshold Alert

To set up the threshold alert:

1. In the navigation panel, select File Replicator > Set Threshold Alert.
2. Select the Mirroring Buffer Threshold 1.

   This is the percentage of mirror buffer usage that triggers the first alert. The default value is 70 percent. This means that when the mirror buffer is 70 percent full, an alert is automatically issued.
3. Select the Mirroring Buffer Threshold 2.

   This is the percentage of mirror buffer usage that triggers the second alert. The default value is 80 percent.
4. Select the Mirroring Buffer Threshold 3.

   This is the percentage of mirror buffer usage that triggers the third alert. The default value is 90 percent.
5. Select the Alert Reset Interval (Hours).

   This is the amount of time the system waits before re-issuing an alert if the condition re-occurs within the interval.

   For example, if you set the Mirroring Buffer Threshold 1 to be 10 percent and the Alert Reset Interval to two hours, the first alert is issued when the mirror buffer is 10 percent full. The system will not issue the Threshold 1 alert again for the next two hours. If at that time the mirror buffer usage is still beyond the 10 percent threshold (but not beyond Thresholds 2 or 3), the Threshold 1 alert is issued again.

   The default value for this field is 24 hours.

6. Click Apply to save your changes.

Breaking the Connection Between Mirror Servers

To promote a file volume on the mirror server (for example, the file volume on the active server is unavailable), you must first break the mirror connection. Break the mirror connection on the active server rather than on the mirror server as described in the following procedure. However, if the active server is down and you cannot access it to break the connection, you can break the mirror connection from the mirror server instead.

To break a mirror connection between mirror servers:

1. In the navigation panel of the active server, select File Replicator > Manage Mirrors.
2. Select the mirror from the table and click Break.

   You are prompted to confirm that you want to break the mirror connection. Once the mirror connection is broken, it disappears from the mirroring table in this panel. To promote the file volume, you must access the Manage Mirrors panel on the mirror server. For more information, see "Promoting a Mirrored File Volume" on page 131.

Promoting a Mirrored File Volume

In the event that the active server fails, the mirror server provides high availability for mirrored file volumes. To make a mirrored file volume available to network users, you must promote the file volume. You must first break the mirror connection, then promote the mirrored file volume and configure its access rights. Once a mirror connection is broken and the mirrored file volume promoted, the original and mirrored file volumes are completely independent.

Caution: The mirror of a strict compliance-enabled volume cannot be promoted. If you need temporary access to a strict compliance mirror volume, you can export it as a read-only file system without promoting it.

To promote a file volume on the mirror server, you must first break the mirror connection. See “Breaking the Connection Between Mirror Servers” on page 131 for instructions.

To promote a file volume on the mirror server:

1. In the navigation panel of the mirror server, select File Replicator > Manage Mirrors.
2. Click Promote.
3. In the Promote Volume window, select the volume to promote and click Apply.

   It may take several minutes to complete this process. To promote a mirrored file volume, the volume must have reached an In Sync state at some point. If the mirrored file volume was out of sync when it is successfully promoted, the volume will be mounted as a read-only volume. Before write-enabling the volume, run the `fsck` command to make any necessary repairs.

   After you break the mirror connection, the system performs a file system check. If the system finds errors during this check, the file volume promotion process could take longer to complete. Data integrity is not guaranteed if the mirror is out of sync during the promote process.

   After you promote the file volume, you might need to reconfigure access rights. Microsoft Server Message Block (SMB) share information is carried over automatically, but you must configure any Network File System (NFS) file volume access and NFS exports for this file volume again. For more information on setting up NFS exports, see “About Setting Up NFS Exports” on page 118.

Reestablishing Mirror Connections

This section provides information about reestablishing mirror connections. The following subsections are included:

Reestablishing a Mirror Connection

This procedure describes how to reestablish a mirror connection after the active server fails and you promote the file volume on the mirror server. The promoted file volume is now the most up-to-date version and functions completely independently of the out-of-date file volume on the active system. To recreate the mirror connection, you must mirror the up-to-date file volume back to the active server, and then mirror the file volume back to the mirror server as you did originally.

Note: If the mirrored file volume was not promoted, do not follow these instructions. The active system automatically brings the mirror back to an In Sync state when it is back online.

In the examples that follow, *Server 1* is the active server, and *Server 2* is the mirror server.

Reestablishing a mirror connection entails the following steps:

1. Make sure the mirror on Server 1 is broken.

   See "Breaking the Mirror Connection on the Active Server" on page 133.

2. Delete the out-of-date file volume on Server 1.

   See "Deleting the Out-of-Date File Volume From Server 1" on page 134.

3. Mirror the up-to-date file volume from Server 2 back to Server 1. See "Mirroring the Up-to-Date File Volume From Server 2 to Server 1" on page 134.

4. Change the role on Server 2.

   See "Changing Volume Roles" on page 135.

   At this point Server 1 would be active again and Server 2 would be the mirroring target.

Breaking the Mirror Connection on the Active Server

To break the mirror connection on the active server:

1. Open a Web browser window to Server 1.
2. In the navigation panel, select File Replicator > Manage Mirrors.
3. Select the mirror connection you want to break.
4. Click Break.

Deleting the Out-of-Date File Volume From Server 1

To delete the out-of-date file volume from Server 1:

1. In the navigation panel of Server 1, select File Volume Operations > Delete File Volumes.
2. Select the file volume that was being mirrored.

   Because the file volume on the mirror server has been promoted and is now the current version, the file volume on the active server is out of date and must be deleted.

   Caution: Before completing the following step, be sure you are deleting the out-of-date source file volume on the active server. Also, be sure that the up-to-date file volume on the mirror server is verified and promoted first.

3. Click Apply to delete the out-of-date file volume.

Mirroring the Up-to-Date File Volume From Server 2 to Server 1

To mirror the up-to-date file volume from Server 2 to Server 1:

1. Open a Web browser window to Server 2.
2. In the navigation panel, select File Replicator > Manage Mirrors.
3. Click Add.
4. Select the file volume to be mirrored from the Volume pull-down menu.
5. Type the mirroring name of Server 1 in the Mirror Host field.
6. Type the Internet Protocol (IP) address of the Server 1 port used for the mirroring connection.
7. Type the alternate IP address.
8. If you need an administrative password to access Server 1, enter it in the Password field.

   If there is no administrative password, leave this field blank.

9. Type the size of the mirror buffer.

   For more information about the mirror buffer, see "About Sun StorageTek 5320 NAS Appliance Mirroring" on page 123.

Be sure there is no I/O activity to the source file volume on Server 2 during mirror synchronization.

10. Click Apply to create the mirror.

    The mirror creation process begins. When the mirror reaches an In Sync state, an identical copy of the file volume exists on both Server 1 and Server 2.

11. In the Manage Mirrors panel on Server 1, select the promoted file volume then click Change Roles.

    See "Changing Volume Roles" on page 135 for more information.

    You have reestablished the original mirroring connection.

Changing Volume Roles

An administrator can switch roles between an active volume and the mirror volume. Changing volume roles enables the active volume to function as the mirror volume and vice versa; however, the original configuration on each volume remains unchanged. Changing roles is not a disaster recovery function.

Note: The volumes must be 100 percent in sync to change roles.

Changing roles can be initiated in the Manage Mirror panel from the active or mirror server.

To change volume roles:

1. In the navigation panel, click File Replicator > Manage Mirrors.
2. Select a volume in the Volume column.
3. Click Change Roles.
4. Click Yes to confirm.

About the Compliance Archiving Option

This section provides information about the Compliance Archiving option. The following subsections are included:

About Compliance Archiving Software

The Compliance Archiving Software helps a company address business practices and regulatory compliance rulings regarding the retention and protection of information. Such rulings and frameworks for records retention and protection include the Security and Exchange (SEC) Regulation 17 CFR § 240.17a-4 (17a-4), Sarbanes Oxley Act, BASEL II, and numerous data protection and privacy directives.

The Compliance Archiving Software was designed from the ground up in consultation with information-management compliance and enterprise content management industry experts to help address the most stringent requirements for electronic storage media retention and protection. Compliance Archiving Software uses WORM (write once, read many) files in accordance with compliance rules.

When enabling the Compliance Archiving Software, be sure that the NAS server and client clocks are synchronized. You can synchronize the NAS server to an external time source using NTP (see "About Time Synchronization" on page 62). A time difference between a client and the NAS server could cause the server to apply the default retention period when a client requests a retention time shorter than the clock skew.

For a detailed technical overview of the Compliance Archiving Software, see Appendix A.

About Enabling Compliance Archiving

The Compliance Archiving Software is available in both a less stringent form (referred to as "advisory enforcement") and in a stringent form (referred to as "mandatory enforcement").

If the Compliance Archiving Software is activated (see "Activating System Options" on page 121), when you create a volume, you can choose to enable compliance with advisory or mandatory enforcement.

Note: Sun StorageTek 5320 NAS Gateway System configurations support compliance with advisory enforcement but not mandatory enforcement.

Note: Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorageTek 5320 NAS Appliance or Sun StorageTek 5320 NAS Cluster Appliance hardware. In particular, the Sun StorEdge 5300 RAID Expansion Unit arrays must not be connected to any device or network other than a private Fibre Channel connection to the NAS head and any Sun StorEdge 5300 Expansion Unit enclosures.

Note: To ensure the strongest possible enforcement of your data retention policies, you should also provide for the physical security of your Sun StorageTek 5320 NAS Appliance or Sun StorageTek 5320 NAS Cluster Appliance. Software-controlled data retention can be no stronger than the physical safeguards used to control access to the system's hardware.

Caution: You should not enable compliance archiving on volumes that will be used by applications and users that are not aware of the different data retention rules enforced by the Compliance Archiving Software.

The Compliance Archiving Software lets administrators enable compliance archiving on any new volumes they create but only when those volumes are initially created. Follow the instructions in "Creating a File Volume or Segment Using the Create File Volumes Panel" on page 46 to create a compliance-enabled volume.

About Compliance With Mandatory Enforcement

Compliance with mandatory enforcement adheres to data protection, retention, and privacy directives, including the following:

- You cannot destroy a compliance volume with mandatory enforcement.
- You cannot destroy a WORM file until the retention period has been met.
- You can increase or decrease the retention period of a volume, but you can only increase the retention period of a WORM file.
- You cannot restore a WORM file from a checkpoint.

Caution: Once you enable compliance archiving with mandatory enforcement on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled or downgraded to advisory enforcement.

About Compliance With Advisory Enforcement

In contrast to compliance with mandatory enforcement, compliance with advisory enforcementt includes the following:

- An authorized administrator can destroy compliance WORM files and compliance volumes (using the audited delete feature).

  Note: Before a volume is deleted the audit logs within that volume must be retained by being copied to a different file system. Otherwise, those logs will be lost.

- An authorized administrator can increase and decrease retention time.
- An authorized administrator can restore WORM files from a checkpoint (using the audited delete feature).
- Default retention time when shipped from the factory is zero days and can be changed.

  Note: Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See See “Managing Trusted Hosts” on page 246..

  When a compliance-enabled volume with advisory enforcement is upgraded to mandatory enforcement, the default retention period for that volume becomes permanent. This can be changed on the Edit Properties panel.

  Note: Upgrading a compliance-enabled volume with advisory enforcement is not supported for gateway configurations.

Compliance Auditing

This section provides information about compliance auditing. The following subsections are included:

About Compliance Auditing

Compliance auditing provides a text-based log for attempted efforts to modify or delete data (with or without proper authority) and is enabled through the use of the Data Retention Audit Service (DRAS) API, which includes the following features:

- Accountability of changes and attempted changes to retained files
- A logging mechanism through which auditable events are stored
- Protection and preservation of the audit log for the life of the system
- Audit log information in a readily viewable format, and secure access to the audit log via standard system access protocols

The set of auditable events are as follows:

- Retaining a file
- Extending the retention period on a retained file
- Requests to unlink (delete) a retained file
- Requests to write to a retained file
- Requests to rename a retained file
- Requests to remove a directory
- Requests to rename a directory

Note – A request to write to a retained file might not be written to the audit log. This can occur if you use an application that attempts to determine the access permissions before writing to a file. Ultimately, the application does not issue a write request if write permission is not available for a retained file.

About File Size Limitations for Auditing

Compliance volumes reserve an amount of free space to guarantee that auditable operations on the volume can be logged. When the free space remaining on a compliance volume falls below this limit, auditable operations will not be executed. A message will be logged indicating that there is not enough space to execute both the operation and the audit, and a warning email will be sent, if email has been configured on the system.

The audit log for each compliance-enabled volume resides in that volume's root directory. The audit log must be accessed by a root user from a trusted host, or by a Windows domain administrator if you are running CIFS in domain mode. See "Managing Trusted Hosts" on page 246 for more information.

Audit log records are text-based and can be accessed through network protocols, including Network File System (NFS) and Common Internet File System (CIFS). The `.audit$` directory must be included in the share path for the contents to be viewed by clients running Windows 2000 or XP. Refer to "About Shares" on page 104 for details about creating shares.

The audit log format is shown in TABLE 8-3.

TABLE 8-3 Audit Log Format

Field	Length	Description
Version	7	Data Retention Audit Service version number
Serial Number	11	A unique sequence number
Length	5	Length of the audit record
Timestamp	21	Date and time at which the event occurred
TID	11	Thread ID of the thread from which the event was executed
Volume ID	11	Volume ID of the volume on which the audit was performed
Protocol	9	Network protocol through which the operation was requested
Inode	11	File system inode number of the file
Client IP Address	16	The Internet Protocol (IP) address of the client from which the operation was requested
Server IP Address	16	IP address through which the client request was received
UID	11	User credential
GID	11	Primary group credential
Operation	8	The audit event
Status	variable	Result of the operation
Domain	variable	Windows domain that the user belongs to, if available
File/Directory Name	variable	File or directory name, that the operation was performed on, if available
Path/Extra Data	variable	Extra information from the audit, if available

Additional Compliance Archiving Features

For a technical overview of the features and programming interface for the Compliance Archiving Software, see Appendix C.

To change compliance archiving settings, see “Configuring the Compliance Archiving Software” on page 269.

CHAPTER 10

Monitoring the System

This chapter describes the monitoring functions of the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System. System monitoring is closely related to maintenance functions and many of the monitoring functions described here refer to other chapters where action can be taken to alleviate issues shown by the monitoring functions. The monitoring functions also show the completion or status of management or maintenance activities.

This chapter includes the following sections:

SNMP Monitoring

This section provides information about Simple Network Management Protocol (SNMP) monitoring. The following subsections are included:

About SNMP Monitoring

You can conduct Simple Network Management Protocol (SNMP) monitoring by enabling SNMP communications. The Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and Sun StorageTek 5320 NAS Gateway System support SNMP monitoring only (not SNMP management).

To interpret Message Information Blocks (MIB), you need the MIB files. The MIB files are installed with the image in the *boot_directory*/www/data/mib directory. For example, `/cvol/nf1/www/data/mib`.

The MIB files are also available for download from `http://sunsolve.sun.com`. Refer to your network management application documentation for information about how to use these files.

Setting Up SNMP

To set up Simple Network Management Protocol (SNMP):

1. In the navigation panel, select Monitoring and Notification > Configure SNMP.
2. Select the Enable SNMP checkbox to enable SNMP.
3. Enter the SNMP community to which the Sun StorageTek 5320 NAS Appliance belongs in the Server SNMP Community field.
4. In the Contact Info field, enter the name of the person who is responsible for this system.
5. In the System Location field, enter the network location.

   This location can be physical or logical.
6. To add a new target address, enter the following information in an empty row of the SNMP table:
   - **Destination IP Address** – Enter the TCP/IP address for the server you want to designate as an SNMP trap destination in the event of system errors.
   - **Port #** – Enter the port to which the system sends traps. The default value is port 162.
   - **Version** – Choose the SNMP version (either 1 or 2) from the pull-down menu.
   - **Community** – Enter the community string for the trap destination.

- **Enable –** Select the checkbox in this column to enable this target address to become a trap destination.

7. To remove a target address, select the line you want to remove and click the Trash button.
8. Click Apply to save your changes.

Viewing System Status

The Web Administrator graphical user interface displays basic system status when you first access it. The status screens vary somewhat from one model to another, based on the functions and physical characteristics of the model.

The information provided on this screen is helpful when calling Customer Support and can provide the first indication of what has failed in some cases.

To view system status, click the Home button in the toolbar.

The screen provides a read-only display of the data listed in TABLE 10-1.

TABLE 10-1 System Status Display

Name	Display
Name	The server name
Model	The system model
Serial #	The unique serial number of the system
Up Time	The amount of time elapsed since the system was last turned on
CPU Load	The current and peak processor load
OS Version	The version of the operating system on the server
Web Admin Version	The version of the Web Administrator on the system
Head Status	The state of server H1 (Cluster only): NORMAL, QUIET, ALONE
Partner Status	The state of server H2 (Cluster only): NORMAL, QUIET, ALONE
Features Enabled	Any optional features enabled on the system

System Logging

This section provides information about system logging. The following subsections are included:

About System Logging

The system log provides basic information in regard to all system events. The log provides essential information when you are trying to determine what errors occurred and when.

Caution: You must enable remote logging or create a log file on local disk to prevent the log from disappearing on system shutdown. (See "Setting Up Logging" on page 33.) When it first starts, the system creates a temporary log file in volatile memory to retain any errors that might occur during initial startup.

The Display System Log panel displays all system events, warnings, and errors, including the date and time they occurred. This panel automatically displays the most recent system events, and you can use the scroll bar to view earlier events.

Note: Changes to drive configuration (such as removing or inserting a drive) may take up to 30 seconds to appear on the event log. As such, if there are multiple changes within that time frame, some events may not be reported.

The following graphic depicts the Display System Log panel.

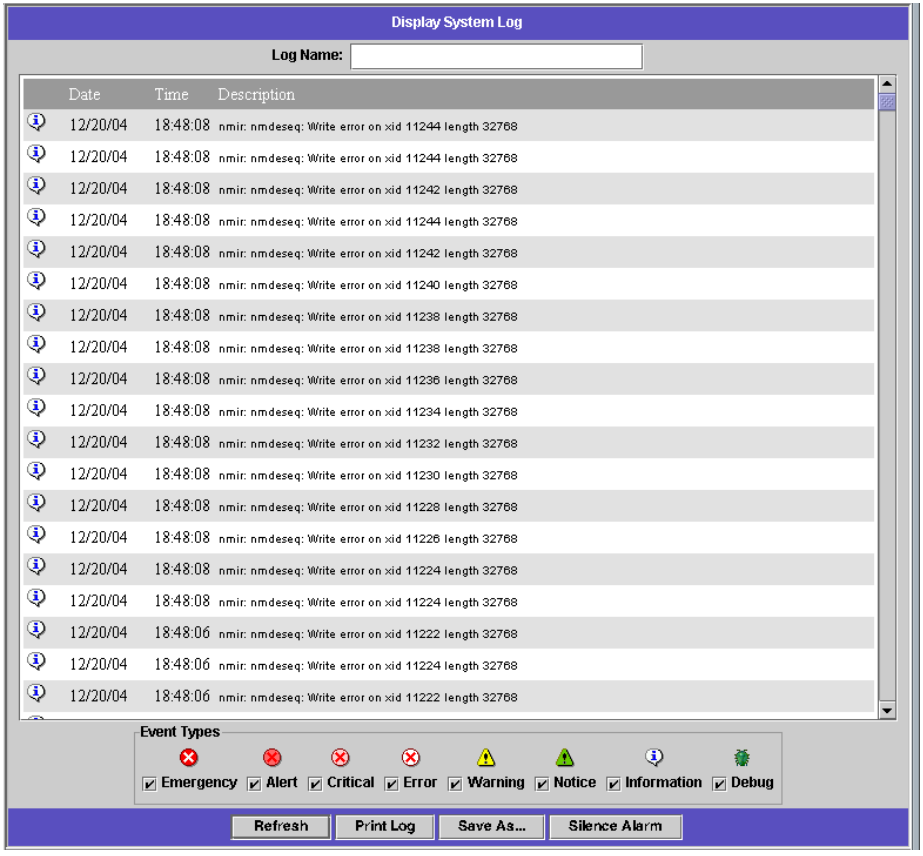


FIGURE 10-1 Display System Log Panel

About System Events

The system log logs eight types of system events. Each event is represented by an icon, shown in TABLE 10-2.

TABLE 10-2 System Event Icons

	**Emergency** – Specifies emergency messages. These messages are not distributed to all users. Emergency priority messages are logged into a separate file for reviewing.
	**Alert** – Specifies important messages that require immediate attention. These messages are distributed to all users.
	**Critical** – Specifies critical messages not classified as errors, such as hardware problems. Critical and higher-priority messages are sent to the system console.
	**Error** – Specifies any messages that represent error conditions, such as an unsuccessful disk write.
	**Warning** – Specifies any messages for abnormal, but recoverable, conditions.
	**Notice** – Specifies important informational messages. Messages without a priority designation are mapped into this priority message.
	**Information** – Specifies informational messages. These messages are useful in analyzing the system.
	**Debug** – Specifies debugging messages.

Viewing the System Log

To view the system log:

1. In the navigation panel, select Monitoring and Notification > View System Events > Display System Log.
2. Check all Event Types you want to view.

   See “About System Events” on page 148 for more information.
3. Click Refresh.

   Note: If your system log contains error messages stating “Unowned SFS2” volumes, call Technical Support for assistance.

System Auditing

This section provides information about system auditing. The following subsections are included:

About System Auditing

System auditing allows the system administrator to audit particular system events by storing records of those events in log files. Auditing is separate from `syslog`; the system audit trail is written to binary files on the local system.

System auditing must be enabled by the system administrator with a file volume configured as the audit trail storage volume. Auditing can be enabled and configured through the Web Administrator graphical user interface, the operator menus, or through CLI commands.

Only a small number of events are audited: system startup, shutdown, disk partition creation and deletion, and volume creation and deletion.

These events are not configurable.

About Audit Configuration

You must specify the audit volume, which can be any non-system volume. Although the system does not force that volume to be used only for auditing, do not use audit volumes for general purpose storage.

The maximum audit log file size has a default value, but it may be changed by the user. Once the current audit log reaches approximately this size (it may vary by about 1 kilobyte), the log file is closed, and a new log file is created.

About Audit Log Files

Audit log files are formatted using date/timestamps as well as the system host name. The current log file will be formatted as *YYYYMMDDhhmmss*`.not_terminated.hostname`.

The timestamps are in Greenwich Mean Time (GMT). For example, if the current log file was started on October 21, 2005 at 1:15 PM GMT on a the Sun StorageTek 5320 NAS Appliance `host =testhost`, the file would be `20051021131500.not_terminated.testhost`.

Once a log file is closed, the name is converted using the same timestamp format. So, if the same log file in the above example reached its maximum size on October 30, 2005 at 7:35 PM GMT, the name would convert to `20051021131500.20051030193500.testhost`.

Audit log files have special attributes. In addition to having zero permissions, they are marked undeletable and immutable, which prevents them from being removed, renamed, or written to by anyone but the system itself. These attributes can be removed by the administrator using the `chattr` command.

Note: Currently, there is no graphical user interface support for reading or removing audit logs. Since the audit logs are stored in binary format, they must be read using the `praudit` command. The `praudit` command converts the binary information in the audit logs into readable text.

Setting Up System Auditing

To set up system auditing:

1. In the navigation panel, select Monitoring and Notification > Configure System Auditing.
2. To enable System Auditing, select the Enable System Auditing checkbox.
3. Select a volume for storing system auditing logs.

   Selectable volumes are non-system volumes. You must create special purpose audit volumes. (For instructions, see "Creating a File Volume or Segment Using the Create File Volumes Panel" on page 46.)
4. Enter the maximum audit log file size, from 1 to 1024 megabytes.

The log file will grow from 0 megabytes to the specified maximum size before creating a new audit log file. The existing audit log files will not be removed. When the volume reaches the 90 percent threshold, alerts are sent and no more log files are written.

5. Click Apply to save your settings.

Viewing Environmental Status

You can view information about the system fan, temperature, power supply, and voltage use.

The following sections are included:

Viewing Fan Status

To view the operational status and revolutions per minute (RPM) of all fans in the Sun StorageTek 5320 NAS Appliance head unit, select Monitoring and Notification > View Environmental Status > View Fan Status.

The View FAn Status panel shows the current status of each fan. A green diamond in the Status column indicates that the fan RPMs are normal. A red diamond indicates that the RPMs have exceeded the acceptable range. If the RPMs of any fan fall below 1800 or if a fan has failed, an email is sent to the designated recipients. For more information on setting up email notification, see "Setting Up Email Notifications" on page 32.

Viewing Temperature Status

To view temperature status, select Monitoring and Notification > View Environmental Status > View Temperature Status in the navigation panel.

The View Temperature Status panel displays the temperature of the sensors in the head unit. A green diamond in the Status column indicates that the unit is operating within the normal temperature range. A red diamond indicates that the temperature has exceeded the acceptable range. If the temperature rises above 55° Celsius (131° Fahrenheit), an email message is sent to the designated recipients. For more information on setting up email notification, see "Setting Up Email Notifications" on page 32.

Note: You cannot change the temperature thresholds.

Viewing Power Supply Status

To display power supply status, select Monitoring and Notification > View Environmental Status > View Power Supply Status in the navigation panel.

The View Power Supply Status panel has three columns showing power supply status. The Status column shows whether the power supply is functioning normally. The Voltage Warning and Temperature Warning columns show whether the voltage and temperature are at acceptable levels.

A green diamond in any of these columns indicates that the voltage or temperature levels are normal. A red diamond indicates that the voltage or temperature have exceeded the acceptable range. In this case, an email notification is sent to designated email notification recipients. For more information about email notification, see "Setting Up Email Notifications" on page 32.

Viewing Voltage Status

To display the current voltage readings, select Monitoring and Notification > View Environmental Status > View Voltage Regulator Status in the navigation panel.

See TABLE 10-3 for the acceptable range for each voltage.

TABLE 10-3 Acceptable Voltage Ranges

Voltage Value	Acceptable Range
Baseboard 1.2V	1.133V to 1.250V
Baseboard 1.25V	1.074V to 1.406V
Baseboard 1.8V	1.700V to 1.875V

TABLE 10-3 Acceptable Voltage Ranges *(Continued)*

Voltage Value	Acceptable Range
Baseboard 1.8VSB (Standby)	1.700V to 1.875V
Baseboard 2.5V	2.285V to 2.683V
Baseboard 3.3V	3.096V to 3.388V
Baseboard 3.3AUX	3.147V to 3.451V
Baseboard 5.0V	4.784V to 5.226V
Baseboard 5VSB (Standby)	4.781V to 5.156V
Baseboard 12V	11.50V to 12.56V
Baseboard 12VRM	11.72V to 12.80V
Baseboard –12V	–12.62V to –10.97V
Baseboard VBAT	2.859V to 3.421V
SCSI A Term Pwr	4.455V to 5.01V
SCSI B Term Pwr	4.455V to 5.01V
Processor Vccp	1.116V to 1.884V

Viewing Usage Information

You can view usage information for file volumes, network activity, system activity, and network ports.The following sections are included:

Viewing File Volume Usage

To view the used and free space of file volumes in the system, in the navigation panel, select Monitoring and Notification > View File Volume Usage.

If usage of a file volume exceeds 95 percent, an email is sent to designated recipients.

Viewing Network Activity

To display the number of I/O requests per second for all Sun StorageTek 5320 NAS Appliance clients, select System Activity > View Networking Activity from the navigation panel.

Viewing System Activity

The Sun StorageTek 5320 NAS Appliance software monitors the activity and load of several devices throughout the storage system. Note that the names and number of devices being monitored varies based on your hardware configuration.

To display the I/O requests for system devices, select System Activity > View System Activity in the navigation panel.

The View System Activity panel lists activity for the system and network devices listed. For more information about the fields on this panel, click the Help button on the panel, or see "View System Activity Panel" on page 365.

Viewing Network (Port) Statistics

To view network (port) statistics:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Configure Network Adapters.

   The Configure Network Adapters panel is displayed.

2. Select the port from the Adapter list.

   The Interface tab Statistics tabs display detailed statistics about the selected port. For more information, see "Configure Network Adapters Panel" on page 350.

Viewing Network Routes

Click a link below for information about network routes and how to view them:

About Network Routes

There are two different kinds of routes: network routes and host routes. Network routes are used to send packets to any host on a particular network. Host routes are rarely used and are implemented to send packets to a host that is not attached to any known network only to another host or gateway.

The following are some examples of route flags shown in the routing table:

- **0x1** – Indicates that the route is usable.
- **0x2** – Indicates that the destination is a gateway.
- **0x4** – Indicates that the destination is a host entry.
- **0x8** – Indicates that the host or network is unreachable.
- **0x10** – Indicates that the destination was created dynamically.
- **0x20** – Indicates that the destination was modified dynamically.

Some flags may be the sums of individual indicators. For example, 0x3 would represent the route as being usable (0x1) and a gateway (0x2), as the sum of these two values.

Displaying Routes

To view the status of all routes in the local network, select Network Configuration > View the Routing Table in the navigation panel.

The View the Routing Table Panel is displayed.

Monitoring System Status

You can monitor Uninterruptible Power Supply (UPS), controller, and mirror status. For more information, see the following sections:

About UPS Monitoring

If you installed the unit with an uninterruptible power supply (UPS), you can monitor the UPS.

Note: You must connect the UPS to the Sun StorageTek 5320 NAS Appliance system before you enable UPS monitoring. Otherwise, the monitoring system notifies you that there is a UPS failure. Also, the Sun StorageTek 5320 NAS Appliance does not support UPS management, only UPS monitoring. Refer to "Connecting to an Auxiliary Local UPS" on page 293 for details about using the UPS.

UPS monitoring provides notification in the event of the following occurrences:

- **Power failure** – Indicates that a power failure occurred and the system is operating on battery power.
- **Power restoration** – Indicates that power was restored.
- **Low battery** – Indicates that the battery is low on power.
- **Recharged battery** – Indicates that the UPS has charged the battery to a normal level.
- **Battery replacement** – Indicates that the UPS has detected a battery defect such that replacement is necessary.
- **UPS alarms** – Indicates that the UPS has detected an ambient temperature or humidity outside of safe thresholds.
- **UPS failure** – Indicates that the system is unable to communicate with the UPS.

You are notified of all errors (except recharged battery) through an error notification email, notification to the Simple Network Management Protocol (SNMP) server, display on the LCD panel, and display in the system log. The recharged battery notification is sent through email, SNMP notification, and system log display only (not LCD panel notification).

Enabling UPS Monitoring

To enable uninterruptible power supply (UPS) monitoring:

1. In the navigation panel, select Monitoring and Notification > Enable UPS Monitoring.
2. Select Enable UPS Monitoring.
3. Click Apply to save your change.

Viewing Controller Information

The read-only View Controller Information panel displays the RAID controller vendor, model, and firmware release.

To view controller vendor, model, and firmware release information, select RAID > View Controller Enclosure Information in the navigation panel.

About Monitoring Mirror Status States

The status of a mirror is displayed in the Manage Mirrors panel and the mirror status states including the following:

- **New** – A new mirror is being created.
- **Creating mirror log** – The mirror buffer is being initialized.
- **Connecting to host** – The active server is connecting to the remote mirror server.
- **Creating extent** – The mirror server is creating disk partitions.
- **Ready** – The system is ready and waiting for the other system to be ready.
- **Down** – The network link is down.
- **Cracked** – The mirror is cracked.
- **Syncing Volume** – The mirror server is synchronizing the file volume.
- **In Sync** – The mirror is in sync.
- **Out of Sync** – The mirror is out of sync.
- **Error** – An error has occurred.

Viewing Mirroring Status

The Sun StorageTek 5320 NAS Appliance software maintains a variety of network statistics for mirrored file volumes. These statistics are available on the active server and mirror server for each mirrored file volume.

To view mirror statistics:

1. From the navigation panel, select File Replicator > View Mirror Statistics.
2. Select the file volume you want from the Select Volume list.

   The system displays the following status, incoming transactions, outgoing transactions, mirror buffer, and network statistics information for that mirrored file volume. For more information, click the Help button on the panel, or see "View Mirror Statistics Panel" on page 313.

CHAPTER 11

System Maintenance

This chapter describes system maintenance functions. It includes the following sections:

Setting Remote Access Options

System security features include the ability to set remote access options. You can enable or disable network services used to remotely access the system. You can run the system in Secure Mode for maximum security or you can specifically enable certain remote access features such as Telnet, Remote Login, and Remote Shell.

The secure services are Secure Web Admin, which uses the Secure Socket Layer (SSL) over Hyper Text Transfer Protocol (HTTP), and Secure Shell (ssh).

To set remote access security:

1. In the navigation panel, select System Operations > Set Remote Access.

2. Check the Secure Mode checkbox for maximum security. In secure mode you can enable only Secure Web Admin and Secure Shell by checking the associated checkbox.
3. If you are not using Secure Mode, select the checkbox for each service you want to enable:
   - Web Admin
   - Telnet
   - Remote Login
   - Remote Shell
4. Click Apply.
5. If you have selected Secure Mode, restart the server for the settings to go into effect. For more information, see "Shutting Down the Server" on page 162.

Configuring FTP Access

This section provides information about configuring File Transfer Protocol (FTP) access. The following subsections are included:

About Configuring FTP Access

File Transfer Protocol (FTP) is an Internet Protocol used to copy files between a client and a server. FTP requires that each client requesting access to the server must be identified with a user name and password.

You can set up three types of users:

- **Administrators** who have the user name `admin` and use the same password used by graphical user interface (GUI) clients.

  The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as the "/" symbol.
- **Users** who have a user name and a password specified in the local password file or on a remote network information service (NIS), NIS+, or Lightweight Directory Access Protocol (LDAP) name server.

The user has access to all existing directories and files within the user's home directory. The home directory is defined as part of the user's account information and is retrieved by the name service.

- **Guests** who log in with the user name `ftp` or its alias `anonymous`. A password is required but not authenticated. All guest users have access to all directories and files within the home directory of the `ftp` user.

  Note: Guest users cannot rename, overwrite, or delete files; cannot create or remove directories; and cannot change permissions of existing files or directories.

Setting Up FTP Users

To set up File Transfer Protocol (FTP) users:

1. In the navigation panel, select UNIX Configuration > Set Up FTP.
2. Check the Enable FTP checkbox.
3. Select the type of FTP access by checking the appropriate checkboxes:
   - Allow Guest Access enables access to the FTP server by anonymous users.
   - Allow User Access enables access to the FTP server by all users. This does not include the admin or root user.

     Note: User names and passwords must be specified in the local password file or on a remote network information service (NIS), NIS+, or Lightweight Directory Access Protocol (LDAP) name server.
   - Allow Admin Access enables root access to those in possession of the administrative password (use with caution).

     Note: A root user is a user with UID equal to 0 and the special Sun StorageTek 5320 NAS Appliance user admin.
4. To enable logging, select the Enable Logging checkbox and specify the log file pathname.

   The log file is saved to the exported volume you specify on the NAS server. For example, /vol1/ftplog will save the log file named `ftplog` to the directory `/vol1`.
5. Click Apply to save settings.

Shutting Down the Server

The Shut Down the Server panel enables you to shut down, halt, or reboot the server. (See "Shutting Down the System" on page 265 for information on shutting down the system using Telnet.)

To shut down, halt, or reboot the server:

1. In the navigation panel, select System Operations > Shut Down the Server.
2. Select the type of shutdown that you want to perform. For detailed information about the available shutdown options, click the Help button on the panel, or see "Shut Down the Server Panel" on page 378.

Caution: Check with Technical Support before selecting the Reboot Previous Version option.

3. Click Apply.

Managing File Checkpoints

This section provides information about managing file checkpoints. The following subsections are included:

About File Checkpoints

A checkpoint, otherwise known as a "consistency spot" (or "c-spot"), is a virtual read-only copy of a primary file volume. While the file volume remains in read/write operation, all data existing at the time the checkpoint was created remains available. Checkpoints are used to retrieve mistakenly modified or deleted files and to stabilize backups.

Note: A checkpoint is a virtual copy of the file volume that is stored in the same physical location as the volume itself. It is not an online backup. If the file volume is lost, so are all the checkpoints.

To use file checkpoints, enable checkpoints and create individual checkpoints or checkpoint schedules.

Creating File Checkpoints

You can choose whether to schedule a checkpoint or create one immediately. Refer to "About Scheduling File Checkpoints" on page 164 for information on setting up a regular checkpoint schedule.

In the Manage Checkpoints panel, you can create immediate checkpoints as well as rename and remove existing ones. Unlike scheduled checkpoints, which are created at a pre-determined day and time, you can create immediate checkpoints in this screen at any time.

To manually create a new checkpoint:

1. In the navigation panel, select File Volume Operations > Edit Volume Properties.
2. Select the volume for which you want to create a checkpoint in the Volume Name pull-down menu.
3. Be sure there is a check mark in the Enable Checkpoints box.

   If not, select the box and click Apply.
4. In the navigation panel, select File Volume Operations > Configure Checkpoints > Manage Checkpoints.
5. To create a new checkpoint, click Create.
6. Select the Volume Name for which you want to create a checkpoint from the pull-down menu.
7. Select one of the checkpoint options. For detailed information about these options, click the Help button on the panel, or see "Create Checkpoint Window" on page 323.
8. Click Apply to create the checkpoint.

Scheduling File Checkpoints

This section provides information about scheduling file checkpoints. The following subsections are included:

About Scheduling File Checkpoints

The Schedule Checkpoints panel displays the current checkpoint schedule and lets you add, edit, and remove scheduled checkpoints. For each scheduled checkpoint, this screen displays the file volume name, a description, the scheduled times and day(s), and the amount of time the checkpoint is retained. The Keep time is expressed as the number of days plus the number of hours.

Adding a schedule line causes the system to automatically set up a checkpoint for the times and dates requested.

You can schedule a maximum of five checkpoints per volume. Multiple checkpoints may be specified per schedule.

An example of multiple checkpoints is shown below.

			Days	Hours AM	Hours PM	Keep	
	Enabled	Description	SMTWTFS	M1234567890E	M1234567890E	Days	+ Hours
1.	Y	MTWTF5am5pm	-*****-	-----*------	-----*------	1	0
2.	Y	SunWed1pm	*--*---	----------	-*----------	0	12
3.	Y	MWFmidnight	-*-*-*-	*----------	----------	0	3
4.	Y	Weekend	*-----*	*-----*-----	*-----*-----	0	6
5.	Y	FriEvery2hrs	-----*-	*-*-*-*-*-*-	*-*-*-*-*-*-	0	2

Adding a Checkpoint to the Schedule

To add a checkpoint to the schedule:

1. Enable checkpoints for the file volume.
2. Add the checkpoint to the schedule.

To enable checkpoints for the file volume.

1. In the navigation panel, select File Volume Operations > Edit Volume Properties.
2. Select the volume for which you want to add a checkpoint in the Volume Name pull-down menu.
3. Verify that there is a check mark in the Enable Checkpoints box.

   If there is not, select the box and click Apply.

To add the checkpoint to the schedule:

1. In the navigation panel, select File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. To add a checkpoint to the schedule, click Add.
3. Select the file volume for which you are scheduling checkpoints.
4. Enter a description for the checkpoint.

   This is a mandatory field. You may want to enter information like the time between checkpoints, such as “weekly” or “daily.”
5. Select the number of days and hours to retain the checkpoint in the Keep Days + Hours drop-down boxes.
6. Select the days on which you want the checkpoint to be created.

   To select more than one day from this list, hold the Ctrl key while clicking additional days with the mouse.
7. In the AM Hours list, select the time(s) of day in the morning when the checkpoint is to be created.

   To select more than one item in this list, hold the Ctrl key while clicking additional items with the mouse.
8. In the PM Hours list, select the times of afternoon or night when the checkpoint is to be created.

   To select more than one item in this list, hold the Ctrl key while clicking additional items with the mouse.
9. Click Apply to save your changes.

Editing an Existing Checkpoint Schedule

To edit an existing checkpoint schedule:

1. In the navigation panel, select File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. Select the schedule line you want to edit, and click Edit.

   The information shown on this screen is identical to that in the Add Checkpoint Schedule window, except that you cannot change the volume name.
3. Edit the relevant information.

   For more information, see "Adding a Checkpoint to the Schedule" on page 165.
4. Click Apply to save your changes.

Removing a Schedule Line

To remove a schedule line:

1. In the navigation panel, select File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. Select the schedule line you want to remove by clicking on it, and click Remove.

Renaming a Checkpoint

To rename a checkpoint:

1. In the navigation panel, select File Volume Operations > Configure Checkpoints > Manage Checkpoints.
2. Select the checkpoint you want to rename, and click Rename.

   The Volume Name and Old Name fields are read-only.
3. Enter the New Name for the checkpoint.

   Caution: If you rename an autodelete checkpoint to a common name, the checkpoint will no longer autodelete.
4. Click Apply to save your changes.

Removing a Checkpoint

To remove a checkpoint:

1. In the navigation panel, select File Volume Operations > Configure Checkpoints > Manage Checkpoints.
2. Select the checkpoint you want to remove, and then click Remove.

Sharing File Checkpoints

Checkpoints can be shared, allowing users to access the data that was current when the checkpoint was created.

To share file checkpoints:

1. In the navigation panel, select Windows Configurations > Configure Shares.
2. Click Add.
3. Type the new share name for the checkpoint in the Share Name box.

   The share name is used to access the checkpoint from the network.
4. (Optional) Select the Mac Extensions checkbox.

   The Mac Extensions option is selected by default.
5. Click the Volume Name pull-down menu box and select the checkpoint volume from the list.

   Checkpoint volumes have the `.chkpnt` extension
6. Leave the Directory field blank.
7. If Active Directory Service (ADS) is enabled and configured, type an ADS context in the Container text box.
8. If the following fields and options are available, complete them as follows:
   - User box = 0 Type 0 in the User box.
   - Group box = 0 Type 0 in the Group box.
   - R/W Password and R/O Password boxes = blank

     Checkpoint volumes are read-only.

These fields and options are unavailable if the system is configured for NT Domain mode.

9. Click Apply.

   Notice the new checkpoint is listed as a share in the Configure Share panel.

Accessing File Checkpoints

Users can access checkpoints, allowing them to access the data that was current when the checkpoint was created.

To access a file checkpoint:

1. Using a network station, click the Windows Start menu.
2. Select Run.
3. In the Run window, type the Sun StorageTek 5320 NAS Appliance server Internet Protocol (IP) address and checkpoint sharename.

   For example, type `\\xxx.xxx.xxx.xxx\sharename.`
4. Click OK.

Setting Up NDMP Backups

The Network Data Management Protocol (NDMP) is an open protocol for network-based backup. NDMP architecture lets you use any NDMP-compliant backup administration application to backup your network attached storage device.

Note: The backup administration application should be configured for logon with the user name `administrator` and the password used by the console administrator (command-line interface).

Note: Checkpoints must be enabled for volumes to be backed up by NDMP. Refer to "Creating File Checkpoints" on page 163.

NDMP is not required to run local backups.

To set up NDMP:

1. In the navigation panel, select System Backup > Set Up NDMP.

2. Select the NDMP network interface card (NIC) to be used for data transfer to the backup tape drive.
3. Look at the gateway address that is displayed for each port.

   If the NDMP backup tape device is located on another network, be sure to select the port that connects to the correct gateway.
4. Click Apply.

Updating the Time Zone Database

The Sun StorageTek NAS 5320 Appliance server supports the major world time zones and is designed to adjust the local time in accordance with Daylight Saving Time (DST). Different countries and regions have different needs for daylight and the DST period varies.

Software release 4.10 (minimum) uses the standard database format for the time zones available at `ftp://elsie.nci.nih.gov/pub`.

The following section describes how to update the time zone and DST information on the NAS server.

1. **Download the current time zone database files from `ftp://elsie.nci.nih.gov/pub/`.**

   The time zone database files are distributed as a tar file named `tzdata`*YYYY*`n.tar.gz`, where *YYYY* indicates the year. For example, `tzdata2005n.tar.gz`.
2. **Use `gunzip` and `tar` to extract the database files.**

   The extracted files reference various continents and regions as shown in TABLE 11-1.

   If a file name has more than eight characters, it will be converted to an 8-character file name as it is extracted. The 8-character file name is a limit of the `/cvol` directory. If you download an individual file that has more than eight characters, you must manually rename the file.
3. **Copy the appropriate file to `/cvol/nf1/tz` or `/cvol/nf2/tz`, depending on the current boot directory setting in `/cvol/defstart`.**

   The `defstart` file contains `1` or `2`, which indicates `nf1` or `nf2` respectively.

   The following example, copies the `northamerica` database file to the `nf1` boot directory.

   ```
   cp northamerica /cvol/nf1/tz/northame
   ```

TABLE 11-1 lists the file name and corresponding continent for each database file. For information about time zone abbreviations, see `http://www.timeanddate.com/library/abbreviations/timezones`.

TABLE 11-1 Time Zone Database Files

Fle Name	Continent/Region
africa	Africa
antarctica	Antarctica
asia	Asia
australasia	Australia and Pacific Islands
etcetera	No DST. GMT offsets only
europe	European countries
northamerica	North America
pacificnew	Place holder for presidential election time
solar87	Special time corrections made in 1987 for Saudi Arabia
southamerica	South America

4. **At the CLI, use `zic` to install the time zone database file for your region.**

   For example, the following command installs the northamerica time zones to the `nf1` boot directory:

   ```
   zic /cvol/nf1/tz/northame
   ```

   A server reboot is not required for the new time zones to take effect.

Enabling CATIA V4/V5 Character Translations

The Sun StorageTek 5320 NAS Appliance and Gateway System interoperate with CATIA V4/V5 products (developed by Dessault Systemes).The following sections provide information about the CATIA software:

About CATIA V4/V5 Character Translations

The Sun StorageTek 5320 NAS Appliance and Gateway System interoperate with CATIA V4/V5 products (developed by Dessault Systemes).

CATIA V4 is a UNIX-only product, whereas CATIA V5 is available on both UNIX and Windows platforms. CATIA V4 may use certain characters in file names that are invalid in Windows. When CATIA customers migrate from V4 to V5, V4 files might become inaccessible in Windows if their file names contain invalid Windows characters. Therefore, a character translation option is provided for CATIA V4/V5 UNIX/Windows interoperability.

The translation table is shown in TABLE 11-2.

TABLE 11-2 CATIA Character Translation Table

CATIA V4 UNIX Character	CATIA V5 Windows Character	CATIA V5 Character Description
Curved open double quotation (not shown)	¨	Dieresis
*	¤	Currency sign
/	ø	Latin small letter O with stroke
:	÷	Division sign
<	«	Left-pointing double angle quotation mark
>	»	Right-pointing double angle quotation mark
?	¿	Inverted question mark
\	ÿ	Latin small letter Y with dieresis
|	Broken bar (not shown)	Broken bar

CATIA V4/V5 interoperability support is disabled by default. You can enable the feature either manually through the command-line interface (CLI) or automatically after a system boot.

Enabling CATIA With the CLI

To enable CATIA by using the command-line interface (CLI), issue the command `load catia`.

When using this method, you must re-enable CATIA support after each system reboot.

Enabling CATIA Automatically on Reboot

To enable CATIA automatically on reboot:

1. Edit `/dvol/etc/inetload.ncf` to add the word `catia` on a separate line within the file.
2. Issue the following two CLI commands to restart the `inetload` service:

   ```
   unload inetload
   load inetload
   ```

   If CATIA V4/V5 support was successfully enabled, an entry similar to the following is displayed in the system log:

   ```
   07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
   ```

Updating Sun StorageTek 5320 NAS Appliance Software

Go to `www.sunsolve.sun.com` to obtain the latest softare version. If you are unsure of which version to download, contact Sun Microsystems Technical Support for assistance in getting the appropriate files for your system configuration. Once you have the files, use the Update Software panel to update the Sun StorageTek 5320 NAS Appliance software.

Caution: Do not update system software or redundant array of independent disks (RAID) firmware when the RAID subsystem is in critical state, creating a new volume, or rebuilding an existing one.

The following procedure requires you to reboot the system after the update process is complete. Rebooting the system requires all I/O to be stopped; therefore, plan to update the software during a planned maintenance period.

Note: In a cluster configuration, perform this procedure on both servers in the cluster before you reboot the server. The cluster should be in optimal mode prior to the update.

To update software:

1. In the navigation panel, select System Operations > Update Software.
2. In the Update Software panel, type the path where the update files are located.

   If you need to look for the path, click Browse.
3. Click Update to start the process.
4. When the update process is complete, click Yes to reboot, or click No to continue without rebooting.

   The update does not take effect until the system is rebooted.

Upgrading Array and Drive Firmware Revision Levels

This section explains how to determine current array and drive firmware revision levels and how to upgrade your firmware. It contains the following topics:

Determining If You Need to Upgrade the Firmware

Before you begin a firmware upgrade, decide if an upgrade is required by determining the current firmware revision level for each array component.

You can use the `raidctl profile` command to capture and record the current firmware revision level of each RAID controller unit, expansion unit, controller NVSRAM, and drive. See "Capturing raidctl Command Output" on page 182 for more information.

Upgrading Array and Drive Firmware (Reboot Required)

Use this procedure to upgrade RAID array and drive firmware. This procedure requires you to reboot the NAS server.

If you cannot reboot the NAS server and need to upgrade only array firmware, refer to "Upgrading Array Firmware (No Reboot Required)" on page 176.

The amount of time required to complete a firmware upgrade will vary, depending on your configuration. For example, it takes approximately 50 minutes to upgrade and reboot a single NAS server with two RAID controllers, one Fibre Channel (FC) expansion unit, and one Serial Advanced Technology Attachment (SATA) expansion unit. See TABLE 11-4 to determine how much time to allow for your configuration.

Note: Upgrading drive firmware always requires a reboot of the NAS server.

Note: All drives of each drive type will be upgraded, including those that are already at the firmware level of the current firmware file.

Caution: Do not perform this procedure if a drive has failed and is in the rebuilding state. You can see this information in the system log or from the Web Administrator RAID page.

Before you begin this procedure, make sure that the NAS server software version 4.10 Build 18 (minimum) is installed. Do not attempt to upgrade array and drive firmware for a NAS server that has a previous operating system (OS) version. If the NAS server software is at an earlier version, go to `www.sunsolve.sun.com` to obtain the latest software version.

To upgrade array and drive firmware:

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 NAS client, enable FTP.

For information about how to enable FTP using the GUI, see “About Configuring FTP Access” on page 160. Refer to See “Configuring File Transfer Protocol (FTP) Access” on page 262. if you are using the CLI.

4. Change to the directory to which you downloaded the patch.
5. Use FTP to connect to the NAS server, and log in as the admin user.
6. Enter `bin` for binary mode.
7. At the `ftp` prompt, create the following directories on `/cvol` by issuing 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. Change to the directory you created for the firmware and copy the firmware file (see TABLE 11-3) using the `put` command.

   For example, to load firmware for the RAID controller issue the following commands:

   ```
   cd /cvol/firmware/2882/ctlr
   put SNAP_288X_06120910.dlp
   ```

Note: The firmware file names are truncated after they are copied to their associated directories.

9. Continue to load each firmware file to the appropriate directory.

TABLE 11-3 lists the directory and example firmware file for each component.

TABLE 11-3 Component Firmware Directories and Files

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`
FC expansion unit (EU)	`/cvol/firmware/2882/jbod`	`esm9631.s3r`
SATA EU	`/cvol/firmware/2882/jbod`	`esm9722.dl`
Drive types:		
Seagate ST314680	`/cvol/firmware/2882/drive`	`D_ST314680FSUN146G_0407.dlp`

TABLE 11-3 Component Firmware Directories and Files *(Continued)*

Component	Directory	Example File Name
Seagate 10K	`/cvol/firmware/2882/drive`	`D_ST314670FSUN146G_055A.dlp`
Hitachi 400GB HDS724040KLSA80	`/cvol/firmware/2882/drive`	`D_HDS7240SBSUN400G_AC7A.dlp`
Fujitsu MAT3300F 300GB	`/cvol/firmware/2882/drive`	`D_MAT3300FSUN300G_1203.dlp`
Seagate 10K 300GB	`/cvol/firmware/2882/drive`	`D_ST330000FSUN300G_055A.dlp`

10. Log out of the FTP session.

11. Use Telnet to connect to the NAS server, and log in to a user account with admin privileges.

12. Reboot the system. For a cluster configuration, reboot both servers.

    The following table provides the approximate time needed to upgrade the firmware for each component.

TABLE 11-4 Firmware Upgrade Time

Component	Time to Complete Upgrade
RAID controller	Reboot plus 15 minutes
RAID controller NVSRAM	Reboot plus 5 minutes
FC or SATA EU	Reboot plus 5 minutes
Drives	Reboot plus 1.5 minutes per drive

13. Verify that the new firmware has been loaded by issuing this command:

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

    You can also check the system log for failures.

Upgrading Array Firmware (No Reboot Required)

This procedure upgrades RAID array firmware without requiring a reboot of the NAS server.

Before you begin this procedure, keep the following in mind:

- NAS server software version 4.10 Build 18 (minimum) must be installed. Do not attempt to upgrade firmware to a NAS server that has a previous OS version.
- This procedure is best performed with limited I/O activity. The RAID controller will quiesce I/O during this procedure.

Caution: Do not perform this procedure if a drive has failed and is in the rebuilding state. You can see this information in the system log.

To upgrade array firmware, with no reboot required:

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. Gather the tray ID for each expansion unit (JBOD) that requires a firmware upgrade.

a. From the Web Admin, go to RAID > View Controller/Enclosure Information.

b. Select the appropriate RAID controller from the Controller Information box.

c. Select a tray ID from the Enclosures Information box.

The Firmware Release field displays either `<N/A>` or a firmware revision level, such as `9848`. If the field has a firmware version number, the selected trayID corresponds to the expansion unit (JBOD). This is the tray ID you will need to upgrade the JBOD firmware.

4. Change to the directory to which you downloaded the patch.
5. From a NAS client, enable FTP.

   For information about how to enable FTP using the GUI, see "About Configuring FTP Access" on page 160. Refer to "Configuring File Transfer Protocol (FTP) Access" on page 262 if you are using the CLI.
6. Use FTP to connect to the NAS server, and log in to a user account with admin privileges.
7. Enter `bin` for binary mode.
8. At the `ftp` prompt, create the following directories on `/cvol` by issuing these commands:

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

9. Change to the directory you created for the firmware and copy the firmware file (see TABLE 11-5) using the `put` command.

   For example, to load firmware for the RAID controller issue the following commands:

   ```
   cd /cvol/firmware/2882/ctlr
   put SNAP_288X_06120910.dlp
   ```

10. Continue to load each firmware file to the appropriate directory.

    The following table lists the directory and example firmware file for each component.

TABLE 11-5 Component Firmware Directory and Files

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`
FC EU	`/cvol/firmware/2882/jbod`	`esm9631.s3r`
SATA EU	`/cvol/firmware/2882/jbod`	`esm9722.dl`

11. Log out of the FTP session.

12. Use Telnet to connect to the NAS server, and log in to a user account with admin privileges.

13. Use the `raidctl download` command to load each file to the target directory.

    Note: For `raidctl` command usage, enter `raidctl` with no arguments at the command line.

    To load the RAID controller firmware from the `ctlr` directory to controller 0 and 1, issue the following command:

    ```
    raidctl download type=lsi target=ctlr ctlr=0
    ```

    This example downloads the firmware file to both RAID controllers and removes the file from the directory.

    Note: The `raidctl download` command deletes the component specific firmware file from `/cvol/firmware/2882` after each successful invocation of the command. For example, the `/cvol/firmware/2882/ctlr` file is deleted after each successful invocation of the `raidctl download type=lsi target=ctlr ctlr=0` command. Therefore, you must re-copy the firmware file after upgrading each component (RAID controller unit, controller NVSRAM, expansion unit, and drives) if you have multiple RAID controller or expansion

units. For a cluster configuration with two RAID controller units, the second unit is specified as `ctlr=2` in the command `raidctl download type=lsi target=ctlr ctlr=2.`

To download NVSRAM, issue this command:

```
raidctl download type=lsi target=nvsram ctlr=0
```

To download the firmware located in the `jbod` directory to expansion enclosure 0 in tray 1, issue this command:

```
raidctl download type=lsi target=jbod ctlr=0 tray=1
```

14. Monitor the progress of each download from the Telnet session.

    The approximate time needed to complete each upgrade is as follows:

Component	Minutes per Component
RAID controller	15 minutes
RAID controller NVSRAM	5 minutes
FC or SATA EU	5 minutes

Note: After the upgrades complete, the `telnet` cursor can take up to 5 minutes to return. Wait during this time until the cursor is displayed.

15. Before continuing to the next component, verify in the system log that the download is complete.

    The following example shows output from the system log:

```
Ctrl-

Firmware Download  90% complete
Firmware Download  95% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
nvsram-
```

```
raidctl download type=lsi target=nvsram ctlr=0
Flashing C0 NVSRAM: /cvol/nf2/../firmware/2882/nvsram/n2882-
61.dlp (48068)
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
ESM-
>> raidctl download type=lsi target=jbod ctlr=0 tray=1

Flashing C0 JBOD 1 with
/cvol/nf1/../firmware/2882/jbod/esm9631.s3r (663604)
Firmware Download  20% complete
Firmware Download  30% complete
Firmware Download  50% complete
Firmware Download  60% complete
Firmware Download  90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download  20% complete
10/26/05 10:57:46 I Firmware Download  30% complete
10/26/05 10:57:50 I Firmware Download  40% complete
10/26/05 10:57:54 I Firmware Download  50% complete
10/26/05 10:57:58 I Firmware Download  60% complete
10/26/05 10:58:03 I Firmware Download  70% complete
10/26/05 10:58:08 I Firmware Download  80% complete
10/26/05 10:58:13 I Firmware Download  90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
                    8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives
```

16. After firmware is downloaded to each component,

Upgrading Drive Firmware (Reboot Required)

Use this procedure to upgrade only drive firmware. This procedure requires you to reboot the NAS server.

Note: Upgrading drive firmware always requires a reboot of the NAS server.

Note: All drives of each drive type will be upgraded, including those that are already at the firmware level of the current firmware file.

The amount of time required to complete a firmware upgrade will vary, depending on the number of drives that are installed plus the time it takes to reboot the NAS server. See TABLE 11-4 to determine how much time to allow for your configuration.

Caution: Do not perform this procedure if a drive has failed and is in the rebuilding state. You can see this information in the system log.

Before you begin a drive firmware upgrade, make sure that the NAS server software 4.10 Build 18 (minimum) is installed. Do not attempt to upgrade firmware to a NAS server that has a previous OS version.

To upgrade drive firmware, with a reboot required:

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. Change to the directory to which you downloaded the patch.
4. From a NAS client, enable FTP.

   For information about how to enable FTP using the GUI, see "About Configuring FTP Access" on page 160. Refer to "Configuring File Transfer Protocol (FTP) Access" on page 262 if you are using the CLI.
5. Use FTP to connect to the NAS server and log in as the `admin` user.
6. Enter `bin` for binary mode.
7. At the `ftp` prompt, create the following directory on `/cvol` by issuing this command:

   ```
   mkdir /cvol/firmware/2882/drive
   ```
8. Change to the directory you created for the drive firmware and copy the drive firmware files (see TABLE 11-3) using the `put` command.

For example, to load firmware for the Seagate ST314680 drive issue the following commands:

```
cd /cvol/firmware/2882/drive
put D_ST314680FSUN146G_0407.dlp
```

9. Log out of the FTP session.
10. Use Telnet to connect to the NAS server and log in as the `admin` user.
11. Reboot the system. For a cluster configuration, reboot both servers.

    The approximate time to complete the upgrade is reboot time plus 1.5 minutes for each drive.
12. Verify that the new firmware has been loaded by issuing this command:

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

    You can also check the system log for failures.

Capturing `raidctl` Command Output

You can use the `raidctl profile` command to determine the current firmware revision level of each RAID controller unit, expansion unit, controller NVSRAM, and drive. This section provides instructions in the following procedures:

- "Capturing raidctl Command Output From a Solaris Client" on page 182
- "Capturing raidctl Output From a Windows Client" on page 192

Capturing `raidctl` Command Output From a Solaris Client

To capture `raidctl` command output from a Solaris client:

1. From a Solaris client, type the `script` command and a file name. For example:

   ```
   > script raidctl
   ```
2. Use Telnet to connect to the NAS server.
3. Type the following `raidctl` command to collect the output:

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

For a cluster configuration with two RAID controllers, the second unit is specified as `ctlr=2`, as shown in the following example:

`raidctl get type=lsi target=profile ctlr=2`

4. Type `exit` to close the Telnet session.
5. Type `exit` again to close the file named `raidctl`.

   The following example shows command output, with the command and resulting firmware levels in bold:

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *********
5310 > raidctl get type=lsi target=profile ctlr=0

SUMMARY--------------------------------
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
   Number of standard volumes: 4
   Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
   Standby: 2
   In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
   Firmware version: PkgInfo 06.12.09.10
   NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS --------------------------------
Number of controllers: 2

Controller in Tray 0, Slot B
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
   Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155753
   Date of manufacture: Sat Oct 16 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:49 2006
   Associated Volumes (* = Perferred Owner):
      lun4* (LUN 3)
Ethernet port: 1
      Mac address: 00.A0.B8.16.C7.A7
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.106
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
```

```
 Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
```

```
 Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155741
   Date of manufacture: Sun Oct 10 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:45 2006
   Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
   Ethernet port: 1
      Mac address: 00.A0.B8.16.C6.F9
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.105
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
```

```
 Link status: Down
      Topology: Unknown
      World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

VOLUME GROUPS--------------------------
   Number of volume groups: 4
   Volume group 1 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun1 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 7
      Drive at Tray 0, Slot 6
      Drive at Tray 0, Slot 5
      Drive at Tray 0, Slot 4
      Drive at Tray 0, Slot 3
      Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun2 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 14
      Drive at Tray 0, Slot 13
      Drive at Tray 0, Slot 12
      Drive at Tray 0, Slot 11
      Drive at Tray 0, Slot 10
      Drive at Tray 0, Slot 9
```

```
 Volume group 3 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun3 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 5
      Drive at Tray 11, Slot 4
      Drive at Tray 11, Slot 3
      Drive at Tray 11, Slot 2
      Drive at Tray 11, Slot 1
      Drive at Tray 11, Slot 7
      Drive at Tray 11, Slot 6
   Volume group 4 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun4 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 13
Drive at Tray 11, Slot 12
      Drive at Tray 11, Slot 11
      Drive at Tray 11, Slot 10
      Drive at Tray 11, Slot 9
      Drive at Tray 11, Slot 8
      Drive at Tray 11, Slot 14

STANDARD VOLUMES---------------------------

SUMMARY
   Number of standard volumes: 4
   NAME    STATUS    CAPACITY  RAID LEVEL  VOLUME GROUP
   lun1    Optimal   681   GB    5           1
   lun2    Optimal   681   GB    5           2
   lun3    Optimal   817   GB    5           3
   lun4    Optimal   817   GB    5           4
```

```
DETAILS

   Volume name: lun1
      Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A
      Subsystem ID (SSID): 0
      Status: Optimal
      Action: 1
      Tray loss protection: No
      Preferred owner: Controller in slot A
      Current owner: Controller in slot B
      Capacity: 681 GB
      RAID level: 5
      Segment size: 64 KB
      Associated volume group: 1
      Read cache: Enabled
      Write cache: Enabled
      Flush write cache after (in seconds): 8
      Cache read ahead multiplier: 1
      Enable background media scan: Enabled
      Media scan with redundancy check: Disabled
DRIVES------------------------------

SUMMARY

   Number of drives: 28
      Supported drive types: Fiber (28)
   BASIC:
CURRENT    PRODUCT      FIRMWARE
   TRAY,SLOT  STATUS  CAPACITY   DATA RATE     ID          REV
      0,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
```

```
 11,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307

   HOT SPARE COVERAGE:

      The following volume groups are not protected:

      Total hot spare drives: 2
         Standby: 2
         In use: 0

   DETAILS:

      Drive at Tray 0, Slot 1 (HotSpare)
         Available: 0
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90HWJ00007510RKKV
Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:BA:3E
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: None
         Available: No
```

```
 Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:CA:12
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No

      Drive at Tray 11, Slot 1
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90JEW00007511BDPL
         Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:C8:8B
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No
Drive Tray 1 Overall Component Information
      Tray technology: Fibre Channel
      Minihub datarate mismatch: 0
      Part number: PN 54062390150
      Serial number: SN 0447AWF011
      Vendor: VN SUN
      Date of manufacture: Mon Nov  1 00:00:00 2004
      Tray path redundancy: OK
      Tray ID: 11
Tray ID Conflict: 0
      Tray ID Mismatch: 0
      Tray ESM Version Mismatch: 0
      Fan canister: Optimal
      Fan canister: Optimal
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
```

```
 Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A68475023N0F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Temperature: Optimal
Temperature: Optimal
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: A (left canister)
         Working channel: -1
         Product ID: CSM100_E_FC_S
         Part number: PN 37532180150
         Serial number: SN 1T44462572
         Vendor: SUN
         FRU type: FT SBOD_CEM
         Date of manufacture: Fri Oct  1 00:00:00 2004
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: B (right canister)
         Working channel: -1
```

Capturing `raidctl` Output From a Windows Client

To capture `raidctl` output from a Windows client:

1. Click Start > Run and type `cmd`. Click OK.

2. Right-click at the top of the window and choose Properties.

   The Properties window is displayed.

3. Change the Screen Buffer size (height) to 3000.

4. Click the Options tab and deselect Insert Mode.

5. Use Telnet to connect to the NAS server, and type the following `raidctl` command to collect the output:

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

6. Copy the text to a file using any text editor. For example:

   a. Select the output text and Press Ctrl-C to copy the data.

   b. Open Wordpad by clicking Start > Programs > Accessories > Wordpad.

   c. Click in the window and press Ctrl-V to paste the text.

   d. Save the file.

7. Open the file and search for the current firmware version for each component.

CHAPTER 12

Replacing Server Components

This chapter provides removal and replacement procedures for customer replaceable units (CRUs). It includes the following sections:

Tools and Supplies Needed

The Sun StorageTek 5320 NAS server can be serviced with the following items:

- No. 2 Phillips screwdriver
- Antistatic wrist strap
- Ballpoint pen or other stylus (to press the recessed Power button)
- 8-mm nut-driver (for motherboard replacement)

Powering Off and Removing the Covers

Use the preparatory procedures in this section when you are referred to them from the removal and replacement procedures.

Powering Off the Server

1. **Choose a method for shutting down the server from main power mode to standby power mode. See** FIGURE 12-1**.**
   - **Local shutdown –** Use the LCD Power button to perform a graceful shutdown of the server under operating system control.
   - **Remote shutdown –** From the Web Admin interface, select System Operations > Shut Down the Server to perform a graceful shutdown of the server.

Caution: Do not use the power button to shut down the system. Always use the LCD Power button or remote shutdown procedure described in "Shutting Down the Server" on page 162. Improper shutdown can result in a loss of data.

When main power is off, the Power/OK LED on the front panel will begin flashing, indicating that the server is in standby power mode.

Caution: When you use the LCD power button to enter standby power mode, power is still directed to the service processor and power supply fans. To completely power off the server, you must disconnect the AC power cords from the back panel of the server.

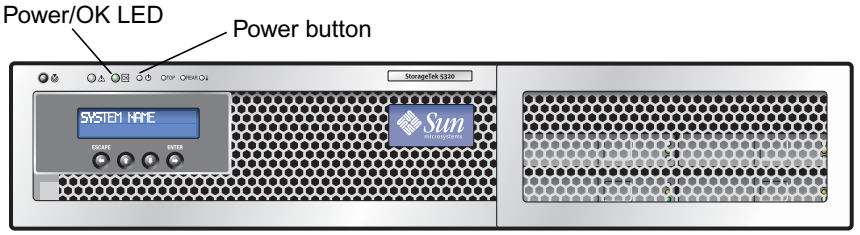


FIGURE 12-1 Power Button and Power/OK LED Location

2. **Unplug both power cords from the server's power supplies.**
3. **Turn off all peripheral devices connected to the system.**
4. **Label any peripheral cables and/or telecommunication lines that you must disconnect in order to remove and replace a specific component.**

Caution: Before handling components, attach an electrostatic discharge (ESD) wrist strap to the grounding post that is built into the back of the chassis. The system's printed circuit boards and hard disk drives contain components that are extremely sensitive to static electricity.

Removing the Main Cover

1. **Press down on the cover release and, using the indent for leverage, slide the main cover toward the back of the chassis, approximately 0.5 inch (12 mm). See** FIGURE 12-2**.**
2. **Grasp the cover by its back edge and lift it straight up from the chassis.**

   Note: When you remove any cover, the intrusion switch that is on the front I/O board automatically powers down the system to standby mode.

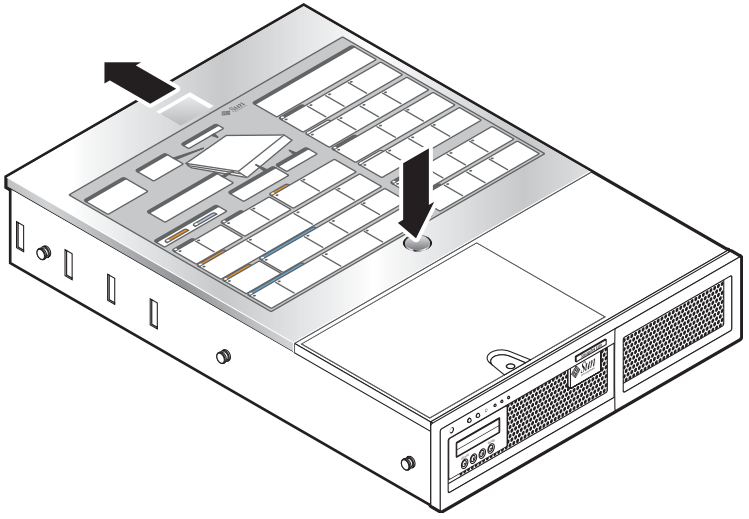


FIGURE 12-2 Removing the Main Cover

Removing the Front Bezel

Remove the bezel from the front of the chassis by following these steps.

1. **Open the fan bay door and use a No. 2 Phillips screwdriver to unfasten the captive screw that locks the bezel in place. See** FIGURE 12-3**.**
2. **Grasp the outer edges of the bezel and gradually ease the bezel away 1 inch (2.4 cm) from the chassis.**

   Caution: A 3-inch USB cable is attached to the LCD on the back side of the bezel. Be careful not to force the bezel from the chassis.

3. **Disconnect the cable from the chassis USB connector.**

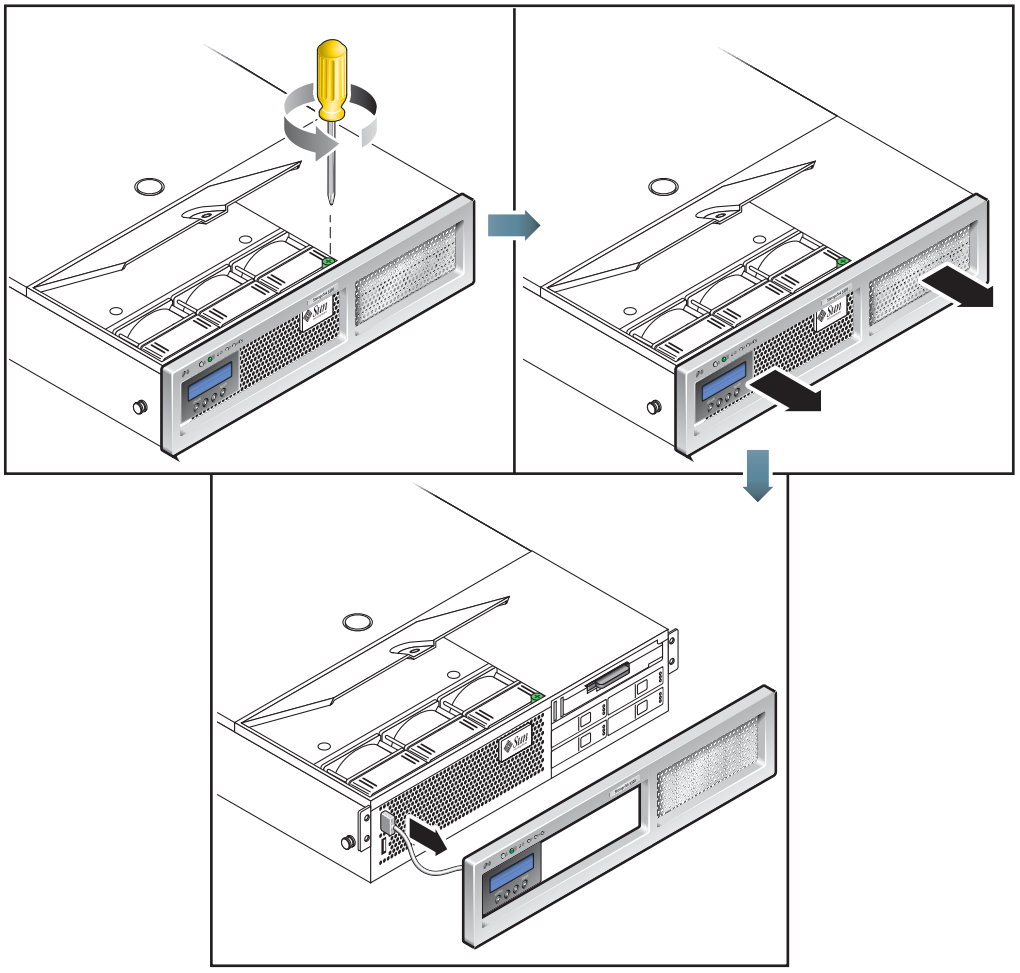


FIGURE 12-3 Removing the Front Bezel

Caution – When the front bezel is removed, the flash disk is accessible. Never remove the flash disk while the server is powered on. The flash disk must be replaced by Sun field service, it is not a customer replaceable unit.

Removing the Front Cover

1. **Open the door to the fan bay. See** FIGURE 12-4**.**
2. **While holding the fan bay door open, slide the front cover toward the front of the chassis approximately 0.25 inch (6 mm).**
3. **Raise the back edge of the cover and then lift it off of the chassis.**

   Note: When you replace the front cover, place the front edge on the chassis first, then set it down into the keyed slots on the chassis sides before sliding it back.

   Note: When you remove any cover, the intrusion switch that is on the front I/O board automatically powers down the system to standby power mode.

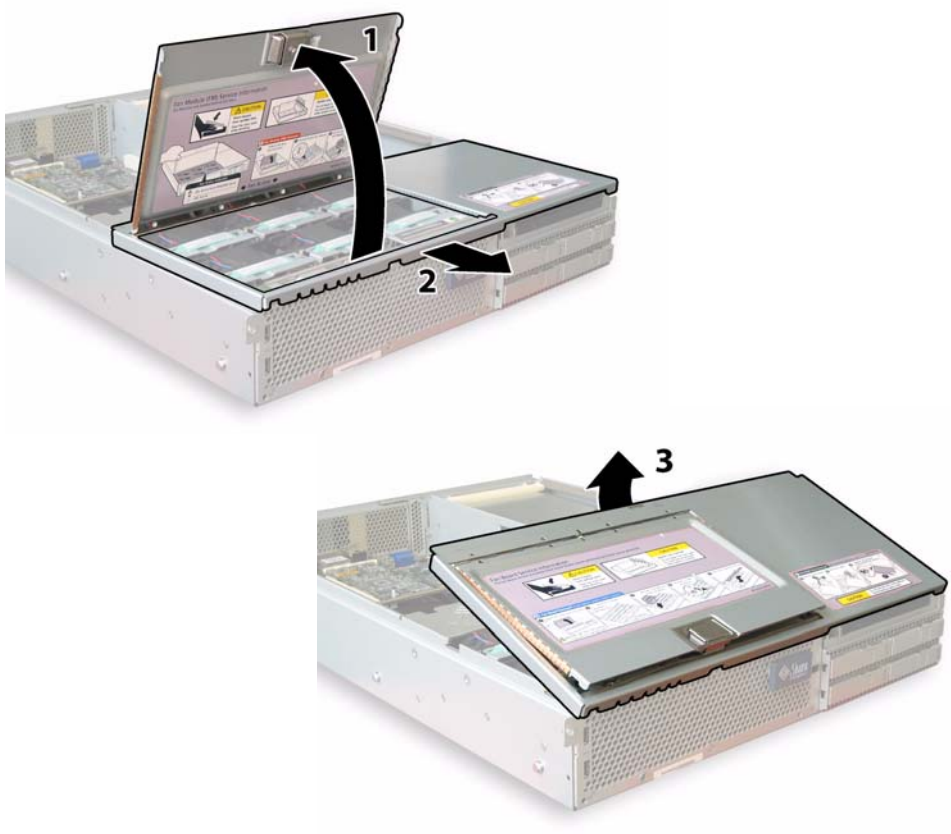


FIGURE 12-4 Removing the Front Cover

Locations of Customer-Replaceable Units

FIGURE 12-5 shows the locations of the customer-replaceable units (CRUs) that are documented in this section.

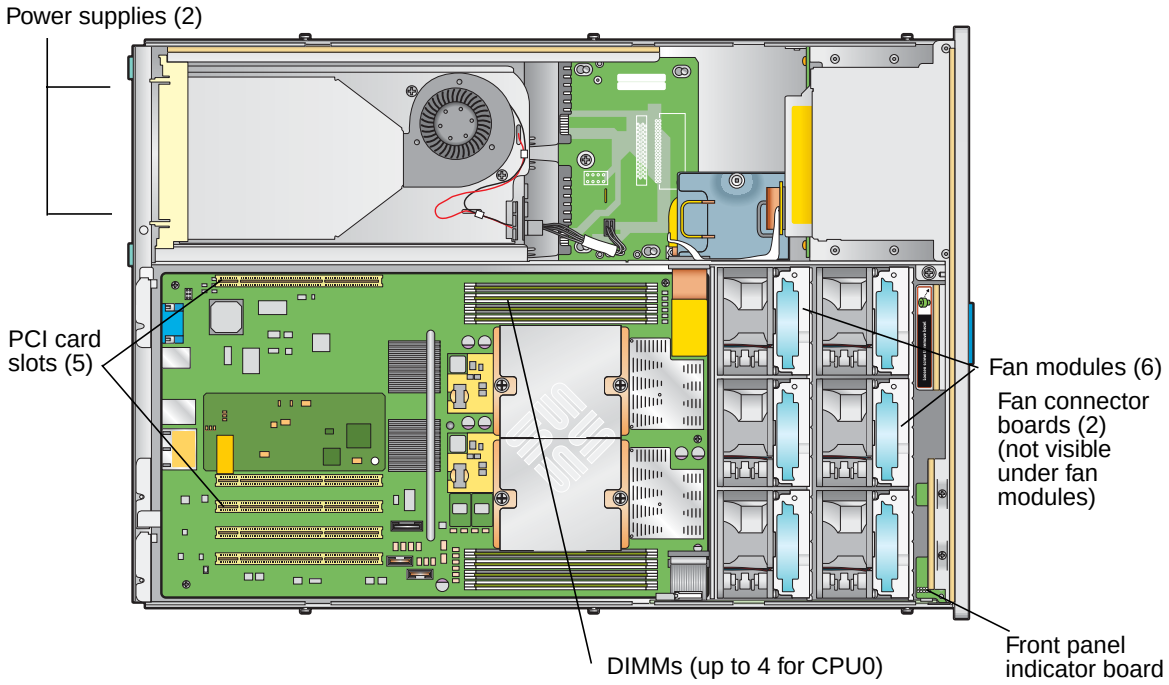


FIGURE 12-5 Replaceable Component Locations

Replacing Components

This section describes removal and replacement procedures for CRUs. Field-replaceable units (FRUs) must be replaced only by trained service technicians. Contact your Sun Service representative for assistance with FRU replacements.

This section contains procedures for replacing the following CRUs:

- "Replacing a Fan Connector Board" on page 201
- "Replacing the Front Panel Indicator Board" on page 204
- "Replacing the Power Supply" on page 205

Replacing a Fan Connector Board

Perform the following steps to remove and replace a fan connector board. There is one supported fan connector board part number 501-6917.

Note: Supported part numbers are subject to change.

1. Power off the server as described in "Powering Off the Server" on page 196.
2. If the server is in a rack, slide it far enough out of the rack so that you can open the fan bay door.

   If you cannot safely view and access the component in this way, remove the server completely from the rack.
3. Open the fan bay door and hold it open. See FIGURE 12-6.

Caution: When you open the fan bay door, be careful to hold it open with one hand so that it does not spring shut and injure your fingers. Do not hold the fan bay door open for more than 60 seconds while the server is running to avoid overheating the server.

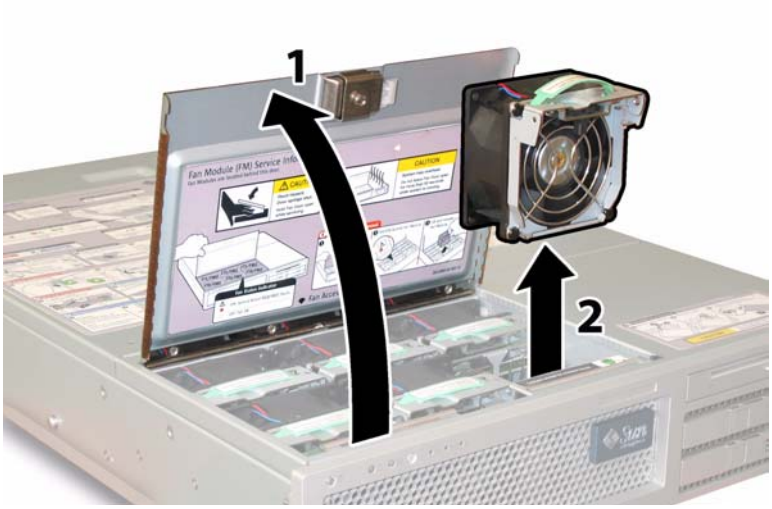


FIGURE 12-6 Opening the Fan Bay Door and Removing a Fan Module

4. Remove the three fan modules that are connected to the fan connector board that you are replacing.

   Grasp each fan module by its plastic strap and lift it straight up out of the fan bay.

5. Remove the single screw that secures the fan connector board to the chassis. See FIGURE 12-7.

Note: In the following figures, the server is shown from the back with the front cover off and all fans removed to provide visibility. Do not remove the covers for this procedure.

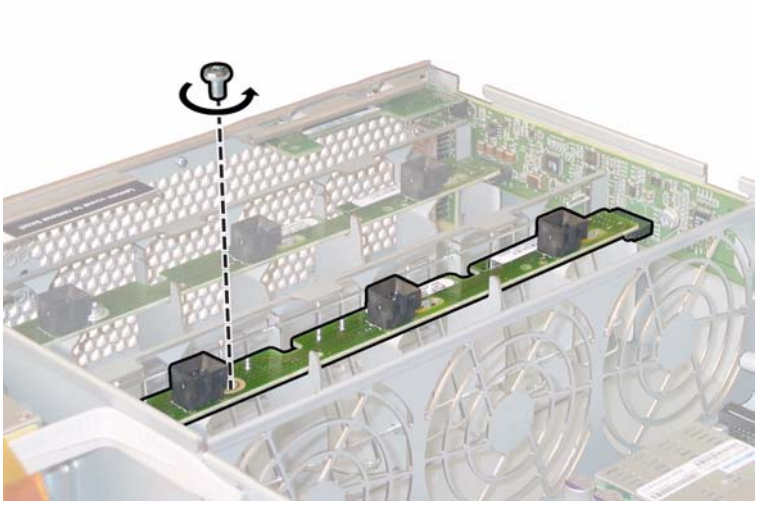


FIGURE 12-7 Removing the Fan Connector Board Securing Screw

6. Slide the fan connector board toward the center of the chassis to disconnect it from the front I/O board and to release it from the two locating tabs on the chassis. See FIGURE 12-8.

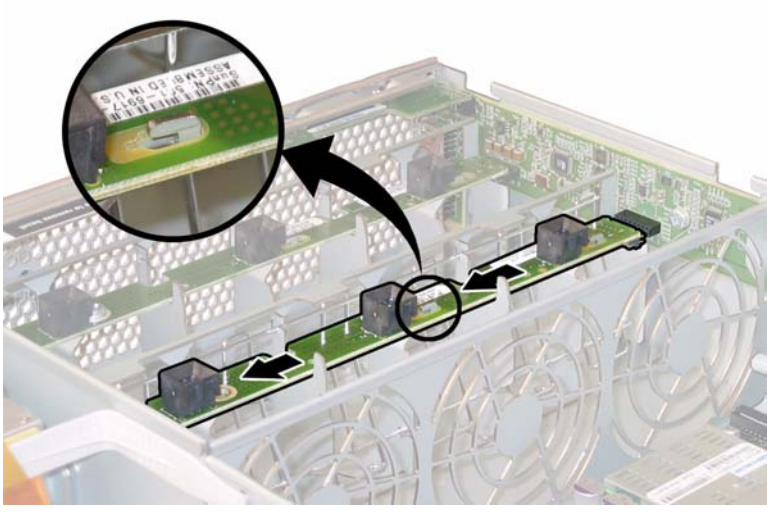


FIGURE 12-8 Releasing the Fan Connector Board

7. Lift the board straight up to remove it from the system.

Installation is the reverse of this procedure.

Replacing the Front Panel Indicator Board

Perform the following steps to remove and replace a front panel indicator board. There is one supported front panel indicator board part number 501-6916.

Note: Supported part numbers are subject to change.

1. Power off the server as described in "Powering Off the Server" on page 196.
2. If the server is in a rack, slide it far enough out of the rack so that you can remove the main cover and front cover.

   If you cannot safely view and access the component in this way, remove the server completely from the rack.
3. Remove the main cover as described in "Removing the Main Cover" on page 197.
4. Remove the front bezel as described in "Removing the Front Bezel" on page 197.

Note: Always unfasten the bezel's securing screw before removing the bezel.

5. Remove the front cover as described in "Removing the Front Cover" on page 199.
6. Remove the two screws that secure the front panel indicator board to the chassis.

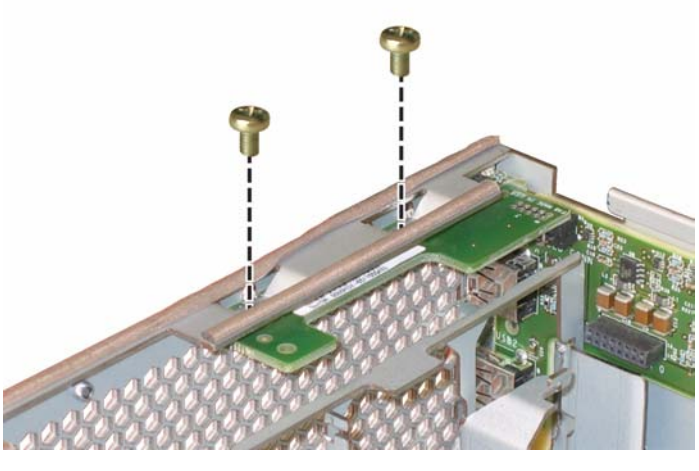


FIGURE 12-9 Removing the Front Panel Indicator Board Screws

7. While supporting the indicator board with your right hand, use your left hand to gently push the indicator board toward the center of the chassis to disconnect it from the front I/O board. See FIGURE 12-10.

FIGURE 12-10 Removing the Front Panel Indicator Board

8. Remove the front panel indicator board from the chassis.

Installation is the reverse of this procedure.

Replacing the Power Supply

Perform the following steps to remove and replace a power supply. There is one supported power supply part number 300-1757.

Note: Supported part numbers are subject to change.

The internal system software designations of the two power supplies in the server are shown in FIGURE 12-11.

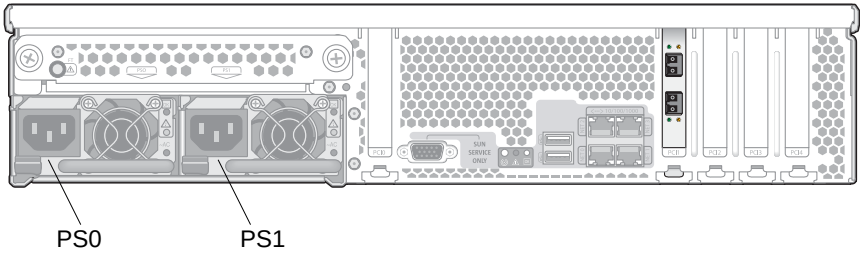


FIGURE 12-11 Designations of Power Supplies

1. Identify which power supply you will replace.

   Each power supply has three LEDs that you can view from the back of the server:

- Top LED: Green indicates that the power supply is operating properly.
- Middle LED: Amber indicates that the power supply is faulty and should be replaced.
- Bottom LED: Green indicates that the AC power source to the power supply is operating properly.

2. Disconnect the AC power cord from the power supply that you are replacing.

   The power supplies are hot-swappable, so you do not have to shut down the server or disconnect the second power supply.

Note: The Service Action Required LEDs on the front panel and back panel blink when a power supply is unplugged. See "Status Indicator LEDs" on page 291 for the LED descriptions.

3. Remove the power supply:

   a. Grasp the power supply handle and push the thumb latch toward the center of the power supply. See FIGURE 12-12.

   b. While continuing to push on the latch, use the handle to remove the power supply from the chassis.

FIGURE 12-12 Removing a Power Supply

Installation is the reverse of this procedure.

When installing a new power supply, press it into the bay until the thumb latch clicks, indicating that it is locked.

Replacing Memory Modules

Perform the following steps to remove and replace the server's dual inline memory modules (DIMMs). There is one supported DIMM, part number 540-6453.

Note: Supported part numbers are subject to change.

Review the following list of memory configuration guidelines before you remove or install any DIMMs:

- The CPU can support a maximum of four DIMMs.
- The DIMM slots are paired, and the DIMMs must be installed in pairs (0 and 1, 2 and 3). See FIGURE 12-13. The memory sockets are colored black or white to indicate which slots are paired.
- CPUs with only a single pair of DIMMs must have those DIMMs installed in that CPU's white DIMM slots (0 and 1).
- Only PC3200 ECC and PC2700 ECC registered DIMMs are supported.
- Each pair of DIMMs must be identical (same manufacturer, size, and speed).

1. Power off the server as described in "Powering Off the Server" on page 196.
2. If the server is in a rack, slide it far enough from out of the rack so that you can remove the main cover.

   If you cannot safely view and access the component in this way, remove the server completely from the rack.
3. Remove the main cover as described in "Removing the Main Cover" on page 197.
4. Locate the DIMM slot on the motherboard in which you will install or replace a DIMM.

Note: To see the fault LEDs in the ejector levers of the DIMM slots, you must put the server in standby power mode, with the AC power cords attached. See "Powering Off the Server" on page 196.

The DIMM ejector LED can indicate a faulty DIMM:

- Off: The DIMM is operating properly.
- On (amber): The DIMM is faulty and should be replaced.

The internal system software designations of the DIMM slots are shown in FIGURE 12-13.

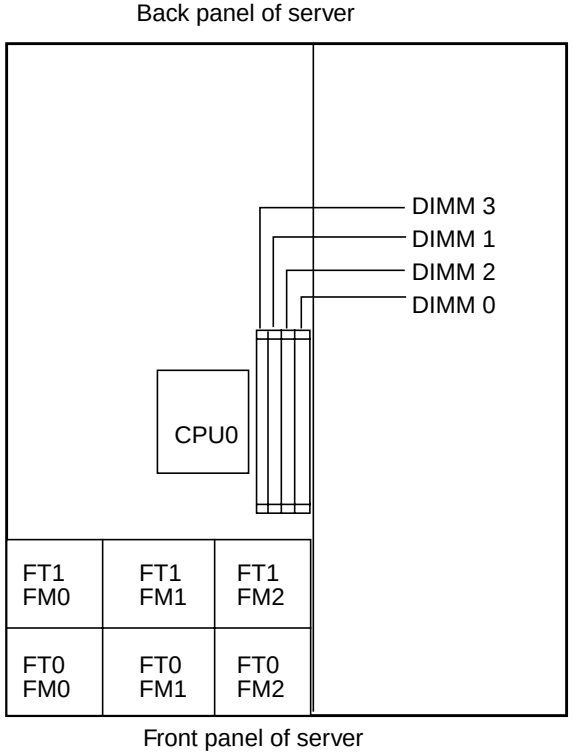


FIGURE 12-13 Designation of DIMM Slots

5. To remove a DIMM:

   a. Rotate both DIMM slot ejectors outward as far as they will go. The DIMM is partially ejected from the socket. See FIGURE 12-14.

   b. Carefully lift the DIMM straight up to remove it from the socket.

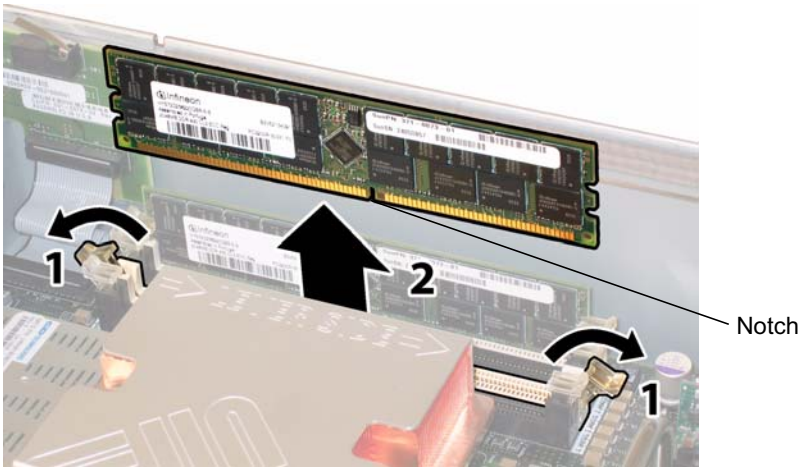


FIGURE 12-14 Removing a DIMM

6. To install a DIMM:

   a. Ensure that the DIMM slot ejectors at both ends of the memory socket are fully open (rotated outward) to accept the new DIMM.

   b. Align the notch in the bottom edge of the DIMM with the key in the DIMM socket. See FIGURE 12-14.

   c. Press down evenly on both top corners of the DIMM until the ejectors snap over the cutouts at the left and right edges of the DIMM.

Replacing a Fan Module Assembly

Perform the following steps to remove and replace an individual fan module. There is one supported fan tray module, part number 541-0269.

Note: Supported part numbers are subject to change.

Caution: The fans are hot-swappable and can be removed and replaced while the system is running. Do not hold the fan bay door open for more than 60 seconds at a time to avoid overheating the server. Remove and replace only one fan at a time.

The internal system software designations of the fan connector boards, or fan trays (FTs), and fan modules (FMs) are shown in FIGURE 12-15.

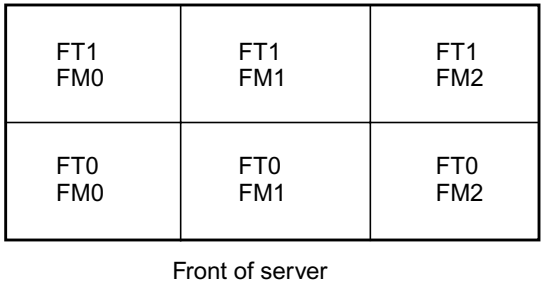


FIGURE 12-15 Designations of Fan Connector Boards and Fan Modules

1. If the server is in a rack, slide it far enough out of the rack so that you can open the fan bay door.

   If you cannot safely view and access the component in this way, remove the server completely from the rack.

2. Open the door to the fan bay and identify the defective fan modules by inspecting the LEDs.
   - Lit: The fan module is faulty and should be replaced.
   - Off: The fan module is operating properly.

Caution: When you open the fan bay door, be careful to hold it open with one hand so that it does not spring shut and injure your fingers. Do not hold the fan bay door open for more than 60 seconds while the server is running to avoid overheating the server.

3. While holding the fan bay door open, grasp the faulty fan module by its plastic strap and lift it straight up out of the fan bay. See FIGURE 12-16.

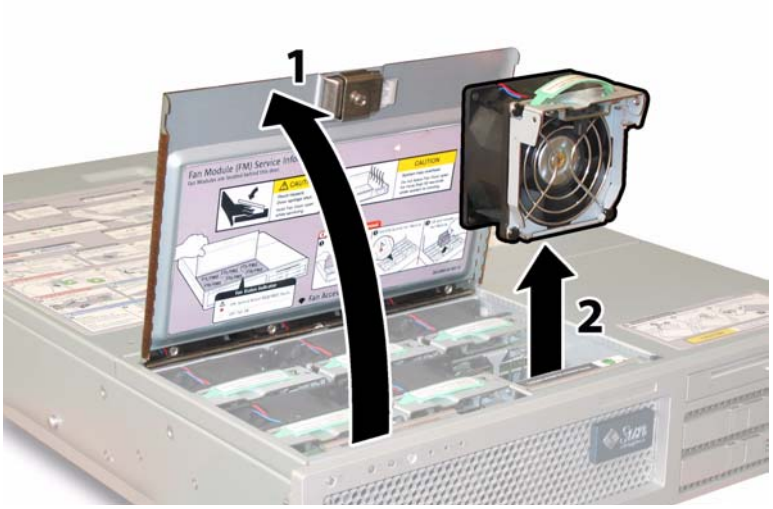


FIGURE 12-16 Opening the Fan Bay Door and Removing a Fan Module

Installation is the reverse of this procedure.

Replacing the Rear Fan Tray

Perform the following steps to remove and replace the rear fan tray (blower tray). There is one supported blower tray, part number 541-0645.

Note: Supported part numbers are subject to change.

1. Working from the back of the server, unfasten the two captive thumbscrews on the face of the rear fan tray. See FIGURE 12-17.

   The internal system software designation of the rear fan tray is `I/O FAN`. The rear fan tray has one fault LED on its face, indicating the following:

   - Off: The fan tray is operating properly.
   - On (amber): The fan tray is faulty and should be replaced.

2. Remove the rear fan tray from the chassis.

   The fan tray cable connector disengages from the internal connector on the chassis.

Note: In FIGURE 12-17, the server is shown with the cover in order to make the component visible; do not remove the cover for this procedure.

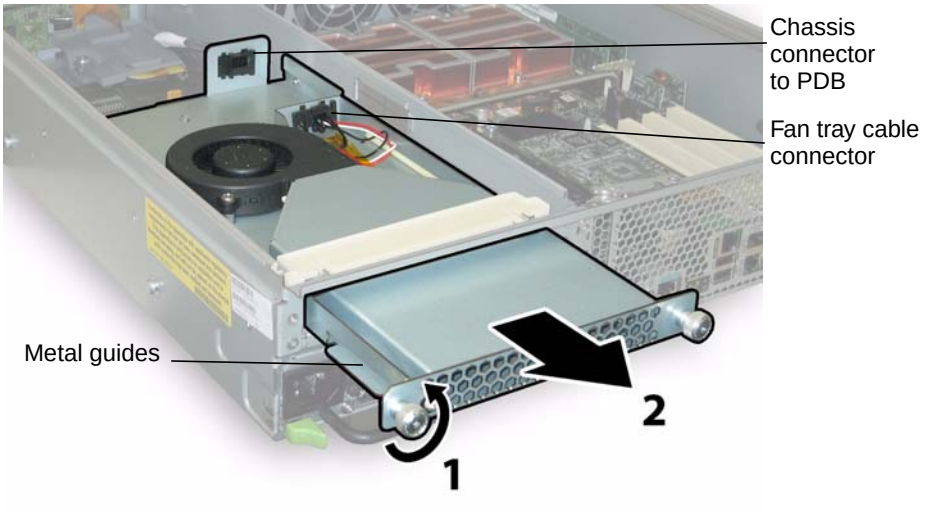


FIGURE 12-17 Removing the Rear Fan Tray

Installation is the reverse of this procedure.

Note: When you reinstall the new rear fan tray, ensure that the metal guides on the fan tray sides (see FIGURE 12-17) engage the plastic rails inside the chassis bay evenly.

Replacing a PCI Card

Perform the following steps to remove and replace a PCI card.

TABLE 12-1 lists the supported part numbers for this component.

Note: Supported part numbers are subject to change.

TABLE 12-1 Supported PCI Card Part Numbers

Component	Part Number
Dual-port Fibre Channel	375-3421
Single-port U320 SCSI HBA	375-3366
NIC Dual Port Fibre	375-3250
NIC Dual Port Cu	370-6687

1. Power off the server as described in “Powering Off the Server” on page 196.
2. If the server is in a rack, slide it far enough out of the rack so that you can remove the main cover.

   If you cannot safely view and access the component in this way, remove the server completely from the rack.
3. Remove the main cover as described in “Removing the Main Cover” on page 197.
4. Locate the PCI card slot in which you will install or replace a PCI card.

   The internal system software designations and the speeds of the five PCI slots are shown in FIGURE 12-18.

   The slots for the PCI-X cards are detected by the system BIOS during bootup in this order: 0, 2, 3, 4, 1.

Note: Before you install a card, consult the manufacturer's documentation for system requirements and configuration information for your specific PCI card.

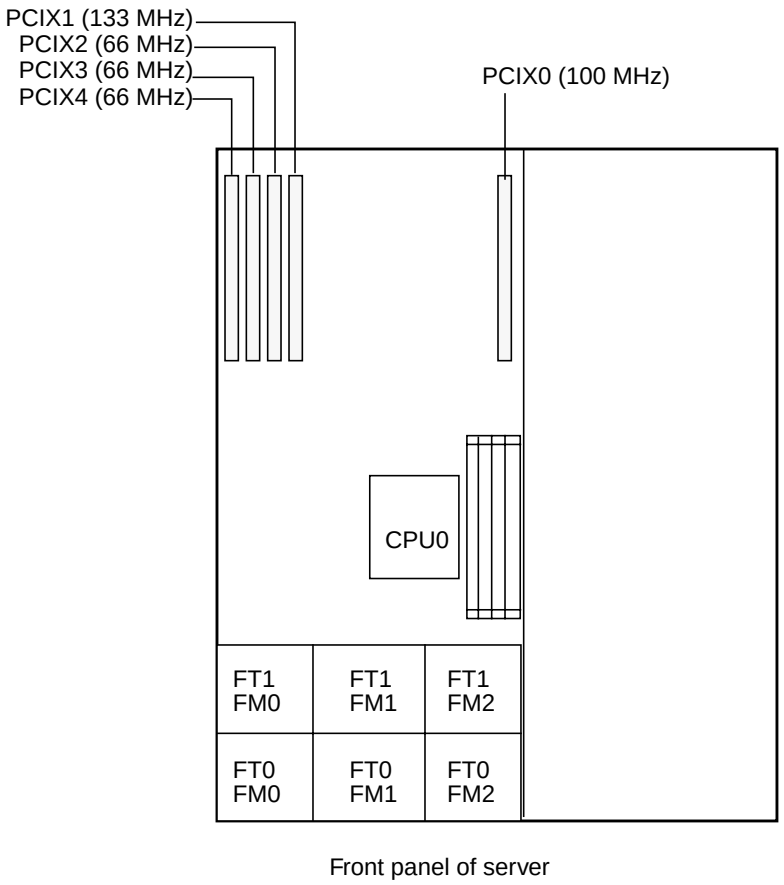


FIGURE 12-18 PCI Slot Designations and Speeds

5. Remove any existing PCI card from the slot:

   a. Disconnect any external cables that are attached to the PCI card.

   b. Working from the back of the chassis, pivot open the PCI card latch that covers the PCI card's back connector panel. See FIGURE 12-19.

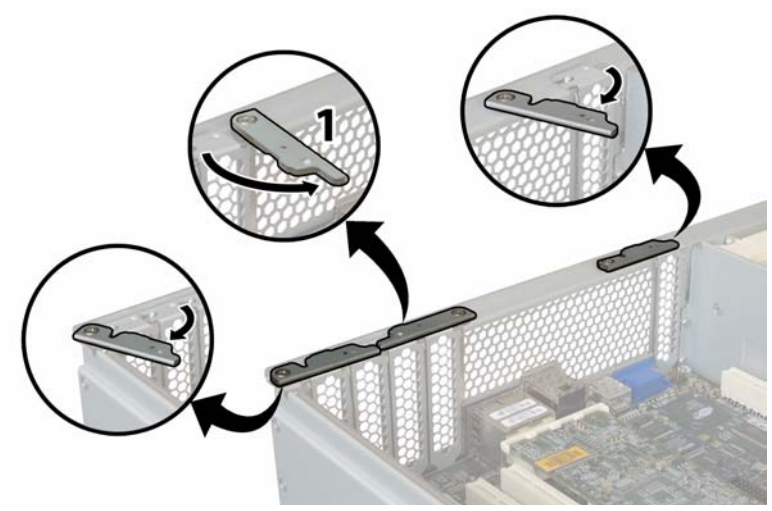


FIGURE 12-19 Opening a PCI Card Securing Latch

c. Pull the PCI card out of the PCI slot. Ensure that the PCI card's back connector panel is released from the tab on the chassis back panel.

6. If there is no PCI card in the slot, remove the PCI-card filler panel from the chassis back panel. See FIGURE 12-20.

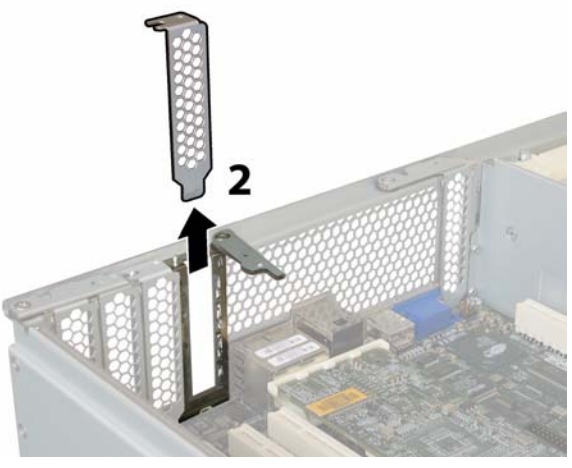


FIGURE 12-20 Removing a PCI-Card Filler Panel

7. Install a PCI card:

a. Working from the back of the chassis, pivot the PCI card latch for the slot open to receive the new PCI card. See FIGURE 12-19.

b. Insert the PCI card into the PCI card slot. Ensure that the PCI card's back connector panel engages the tab in the chassis back panel. See FIGURE 12-21.

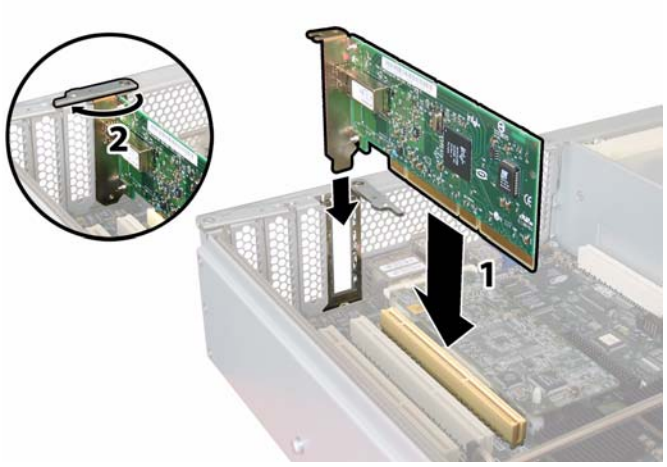


FIGURE 12-21 Installing a PCI Card

c. Pivot the PCI card latch closed over the back connector panel of the PCI card until it locks. See FIGURE 12-21.

APPENDIX **A**

Console Administration

The console is the alternative method to Web Administrator application for managing the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, and the Sun StorageTek 5320 NAS Gateway System. You can use a number of protocols, such as Telnet, SSH, and RLogin to connect to the administrator console as long as the application you use has an ANSI-compatible terminal emulator. In this appendix, the Telnet protocol is used because it is readily available in Windows.

Note: Remote access security settings might need to be altered to access the command-line interface. For remote access details, see "Setting Remote Access Options" on page 159.

This appendix includes the following sections:

Accessing the Console Administrator

In this example, the Windows Telnet Protocol is used to access the Console Administrator command-line interface. However, you can use another protocol as long as it has an ANSI-compatible terminal emulator.

Accessing the Windows Telnet Protocol

To access Windows Telnet:

1. Click Start from your desktop taskbar.
2. Select Run.
3. In the Run window, type `cmd` and click OK.
4. At the command prompt, type `telnet` *ipaddress* where *ipaddress* is the IP address of the server, and press Enter.
5. If administrative access is password-protected, enter the password.

   Once connected, the Telnet screen displays the following command line prompt:

   ```
   connect to (? for list) ? [menu]
   ```

   At this point, you can go directly to the main menu or you can access the command-line interface (CLI) to perform specific commands.

   To access the main menu, press Enter.

Accessing the Console Administrator Command-Line Interface

To access the Console Administrator command-line interface using the Windows Telnet Protocol:

1. At the connection prompt, type `admin` and press Enter.
2. Type the administrative password and press Enter.

The command line prompt appears. You can type a command or select `menu` to access the console's main menu.

Caution: Use commands carefully to avoid unintended results.

To return to the command line, press Esc from the main menu.

Console Menu Basics

Here are a few basic guidelines for using the console:

- To select a menu, press the number or letter associated with the item. For example, press **1** to select 1. Activity Monitor.
- The box at the bottom of every screen displays the tasks you can perform and which letter you need to select to perform the action.
- Use the spacebar to scroll through a list.

The keys used to edit screen fields are listed in the following table

TABLE A-1 Active Screen Keys

Keys	Action
Backspace, Delete, Ctrl+H	Deletes the previous character.
Ctrl+U	Deletes the entire field.
Enter, Ctrl+M, Ctrl+J, Ctrl+I, Tab	Complete the current entry and moves the cursor to the next field.
Esc	Exits the screen with no change.

If you do not want to change a field value, press Enter to move the cursor the next field without changing the information.

Viewing the Main Menu

The main menu consists of the following sections:

- **Operations** – Press any number to perform the corresponding server operation.
- **Configurations** – Press any letter to perform the corresponding server configuration command.
- **Access Control** – Press any letter to set up access to the corresponding menu items.

- **Extensions** – Press any letter to select the corresponding extension. Use the spacebar to scroll through the extension lists.

To use the menu:

1. Select the menu item by pressing the corresponding letter or number.
2. Press the spacebar to view more options under the Extension lists.

Backing Up Configuration Information

After you configure the system, you should create a backup of the configuration.

Caution: The system stores redundant copies of the configuration information, but you must make a backup copy in case of system failure.

In a cluster configuration, perform the following procedure on only one server. The configuration is automatically synchronized between servers; therefore, it is not necessary to create a backup of the configuration on each server.

To back up the configuration information:

1. Follow instructions for "Accessing the Console Administrator" on page 218.

Caution: Use commands carefully to avoid unintended results.

2. At the command line, enter `load unixtools`.
3. Type `cp r v /dvol/etc` *backup path*, where *backup path* is the full path, including the volume name, of the desired directory location of the configuration file backup. The directory must already exist and be empty.

   This copies all of the configuration information stored in the `/dvol/etc` directory to the designated location.

System Management

You can use the console administrator to perform system management tasks. This section describes the following tasks:

- "Configuring TCP/IP" on page 221
- "Modifying the Administrator Password" on page 221
- "Controlling the Time and Date" on page 222

Configuring TCP/IP

To configure TCP/IP:

1. From the Configuration menu, select Host Name & Network.
2. Select 1. Edit fields.
3. Enter the server host name, then press Enter.
4. Enter the Maximum Transfer Unit (MTU), or press Enter to retain the default.
5. Enter the server IP address, then press Enter.
6. Enter the network IP subnet mask, then press Enter.
7. Enter the network IP broadcast, then press Enter.
8. Select 1. Setup to configure alias IP addresses, then press Enter.
9. Repeat steps 3. - 8. for all other ports. Press Enter to continue.

   Note: Use the spacebar to scroll down if additional ports are present.
10. Enter the gateway address, then press Enter.
11. Select 7. Save changes.

Modifying the Administrator Password

To modify the administrator password:

1. From the Access Control menu, select Admin Access.
2. Select Y. Yes to enable password protection, or N. No to disable it.

   Note: Always protect your system with a password.
3. If you select Yes, the system prompts you for a password. Enter the password for administrative access, then type it again to confirm.

4. Select 7. Save changes to activate the new password.

Controlling the Time and Date

Use the Timezone, Time, Date menu option to change time zone, time, and date set on the system. The real-time clock on the mainboard keeps track of local time.

Note: The first time you set the time and date on the system you also initialize the system's *secure clock*. This clock is used by the license management software and the Compliance Archiving Software to control time-sensitive operations.

Caution: Once the secure clock has been initialized, it cannot be reset. Therefore, it is important that you set the time and date accurately when you are configuring the system.

To set the time zone, time, and date:

1. From the Configuration menu, select Timezone, Time, Date.
2. Select the appropriate time zone, then press Enter.
3. Select daylight savings time Y or N.
4. Type the new date, then press Enter.

   The format is YYYYMMDD, where YYYY is the year, MM is the month, and DD is the day. For example, `20041001` equals October 1, 2004.
5. Type the current time, then press Enter.

   The system uses a 24 hour clock.
6. Select 7. Save changes.

   Note: If this is the first time you have set the time and date on the system, this procedure will set the secure clock to the same time and date. Make sure that you set the time and date accurately, because you can only set the secure clock once.

Setting Time Synchronization

You can configure the system to synchronize its time with either the NTP Protocol or an RDATE server.

NTP is an Internet Protocol used to connect and synchronize the clocks of computers to a reference time source. Typical NTP configurations use multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

RDATE servers are normally present on UNIX systems and enable you to synchronize system server time with RDATE server time.

Setting UP NTP for Time Synchronization

To set up NTP:

1. From the Extensions menu, select NTP Configuration.
2. Select 1. Edit fields to configure NTP settings.
3. Select Y. Yes to enable NTP.
4. You can configure up to two NTP servers. Select Y. Yes to enable the first NTP server.
5. Enter the name or IP address of the first NTP server the Sun StorageTek 5320 NAS Appliance polls for the current time, then press Enter.
6. Choose the type of Authentication to use, either 0. none or 1. symmetric-key.

   Symmetric key authentication support lets the Sun StorageTek 5320 NAS Appliance verify that the NTP server is known and trusted by using a key and key ID. The NTP server and Sun StorageTek 5320 NAS Appliance must agree on the key and key ID to authenticate their messages.
7. If you select Symmetric Key as the authorization scheme in the previous field, enter the Key ID associated with the private key from the key file to be used with this NTP server.

   The valid range for this value is 1 to 65534.
8. To configure a second NTP server, repeat steps 4. - 7. for Server 2.
9. In the Min. Polling Interval field, enter the minimum polling rate for NTP messages.

   This value, raised to the power of two, is the minimum number of seconds of the polling interval. For example, entering 4 results in 16 seconds between polls. The valid range for this field is 4 to 17.
10. In the Max. Polling Interval field, enter the maximum polling rate for NTP messages.

This value, raised to the power of two, is the maximum number of seconds of the polling interval. For example, entering 4 results in 16 seconds between polls. The valid range for this field is 4 to 17, but must be larger than the minimum polling interval.

11. In the Broadcast Client Enabled field, select Y. Yes for the Sun StorageTek 5320 NAS Appliance to respond to server broadcast messages received on any interface.
12. In the Require Server authentication field, select Y. Yes to require authentication for servers using the Broadcast client.

    NTP servers not using authentication will not be accepted.
13. Select 7. Save changes.

Setting Up the RDATE Server and Tolerance Window for Time Synchronization

To set up the RDATE server and tolerance window:

1. From the Extensions menu, select RDATE time update.
2. Select 1. Edit fields.
3. Enter the RDATE server name or IP address, and press Enter.
4. Enter the tolerance.

   If the Sun StorageTek 5320 NAS Appliance system time is different than RDATE server time by less than this number of seconds (+ or –), Sun StorageTek 5320 NAS Appliance system time is synchronized with RDATE server time. This check occurs every day at 11:45p.m. Press Enter.
5. Select 7. Save changes.

   If you have an anti-virus scan engine running on your network, you can configure anti-virus protection on the system. For more detail about anti-virus protection, see "About Anti-Virus Software" on page 65.

Enabling Anti-Virus Protection Through the Command-Line

To enable anti-virus protection:

1. From the Extensions menu, select Anti-Virus Configuration.
2. Select 1. Edit fields.
3. In the AVA Enable field, enable anti-virus protection by specifying Yes.
4. In the Scan mode field, select the scan mode.

   For details about scan mode options, see "Enabling Anti-Virus Protection" on page 65.
5. Specify the TCP/IP address of the scan engine to use.
6. Specify the TCP/IP port number on which the ICAP server listens for connections; typically port 1344.
7. Specify the maximum number of concurrent file scan operations that your system will dispatch to the scan engine; typically 2.
8. Specify the file types to include and exclude as well as any exempt clients, groups, or shares.

Specification	Description	Format
File Types Included	Each file type extension to include. Leave blank to include all.	Three or fewer characters, comma-separated. May use ? for wildcard matching.
File Types Excluded	Each file type extension to exclude from scanning.	Three or fewer characters, comma-separated. May use ? for wildcard matching.
Exempt Clients	Name or IP address of each client exempt from scanning.	Comma-separated.
Exempt Groups	Name of each Windows/NT or Windows Active Directory group (not UNIX groups) exempt from scanning.	May include spaces, comma-separated.
Exempt Shares	Name of each CIFS share exempt from scanning. Note: administrative shares (X$) are always exempt from scanning.	Comma-separated.

9. Select 7. Save Changes.

Selecting a Language Through the Command-Line

You can specify the language for NFS and CIFS.

To select a language:

1. From the Extensions menu, select Language Selection.
2. Type the desired language then press Enter.

   The languages that are supported are listed at the top of the screen.

Managing Routes

The routing table contains a list of network paths by which the system sends network packets to specified destinations. Each route entry consists of a destination address and a path. The destination is either a network or a host. The path is the gateway device through which the packet reaches its destination.

To manage static routes in the local network:

1. From the Configuration menu, select Host Name & Network.
2. Select 2. Manage Routes.
3. Select 1. Add route, then select 1. Edit.
4. Select whether the route type is for a host, network, host through a gateway, or network through a gateway.
5. Enter the destination IP address, then press Enter.
6. Enter the path or gateway address used to connect the Sun StorageTek 5320 NAS Appliance with its destination, then press Enter.

   The gateway device must connect to the same subnet as the Sun StorageTek 5320 NAS Appliance.
7. Select 7. Save Changes.

Name Services

The name, services, and functions available through the console interface vary from those available through the GUI.

Setting Up DNS, `syslogd`, and Local Logging

The domain name system (DNS) is a hierarchical name system that translates domain names into IP addresses. `syslogd` is a utility that provides support for remote logging. You can only enable remote logging if you have a UNIX system with the `syslogd` utility on the network that can receive the Sun StorageTek 5320 NAS Appliance system log. All of these functions are set up on the same screen.

After the `syslogd` utility is set up, all log messages are sent to the selected server. This allows you to centralize a record of log messages from all the servers onto one system.

To set up DNS, Dynamic DNS, `syslogd`, and local logging:

1. From the Configuration menu, select DNS & SYSLOGD.
2. Select 1. Edit fields.
3. Select Y. Yes to enable DNS.
4. Enter the IP address for the DNS server to be consulted first for name resolution, then press Enter.
5. Enter the IP address of the server to be consulted second for name resolution, then press Enter.

   If you do not have a secondary DNS server, leave this field blank.
6. Enter the domain name of the DNS server, then press Enter.
7. Enter the maximum number of times the system should attempt a DNS query for each DNS server, then press Enter.
8. Enter the number of seconds of delay between attempts to query each DNS server, then press Enter.
9. Select Y. Yes to enable remote logging. If there is no `syslogd` server on the network, select N. No and skip to step 15.

This feature lets the Sun StorageTek 5320 NAS Appliance send log messages to a remote `syslogd` server.

10. Enter the `syslogd` server name or IP address, then press Enter.
11. Select the appropriate facility, then press Enter. The facility identifies the application or system component generating the messages. Facilities include:
    - **Kern** – Messages generated by the kernel. These cannot be generated by any user processes.
    - **User** – Messages generated by random user processes. This is the default facility identifier if none is specified.
    - **Mail** – The mail system.
    - **Daemon** – System or network daemons.
    - **Auth** – Authorization systems, such as login.
    - **Syslog** – Messages generated internally by syslogd.
    - **Local0–Local7** – Reserved for local use.
12. Select the type of system events for the Sun StorageTek 5320 NAS Appliance logs:
    a. Select the appropriate event type.
    b. Select Y. Yes to enable reporting of events of that type. Event types include:
    - **Emerg** – Specifies emergency messages. These messages are not distributed to all users. Emerg priority messages can be logged into a separate file for reviewing.
    - **Alert** – Specifies important messages that require immediate attention. These messages are distributed to all users.
    - **Crit** – Specifies critical messages not classified as errors, such as hardware problems. Crit and higher-priority messages are sent to the system console.
    - **Err** – Specifies any messages that represent error conditions, such as an unsuccessful disk write.
    - **Warning** – Specifies any messages for abnormal, but recoverable, conditions.
    - **Notice** – Specifies important informational messages. Messages without a priority designation are mapped into this priority message.
    - **Info** – Specifies informational messages. These messages are useful in analyzing the system.
    - **Debug** – Specifies debugging messages.

    c. Press Enter to move to the next event type.
13. Select Y. Yes to enable Dynamic DNS updates.

    These updates enable nonsecure dynamic updates to occur during bootup.

14. To enable secure updates, enter the name of a Windows user with whom the dynamic DNS client can verify updates, then press Enter.

    This user must have administrative rights.

15. Enter the password of the Dynamic DNS user, then press Enter.

16. Enter Y. Yes to enable local logging.

17. Enter the log file path (directory) and file name in the Log File field.

    Note: You cannot set up local logging to the `/cvol` directory. Specify another directory such as `/dvol/error.txt`.

18. Enter the maximum number of archive files in the Archives field.

    The allowable range is from 1 to 9.

19. Type the maximum file size in kilobytes for each archive file in the Archives field.

    The allowable range is from 1000 to 999,999 kilobytes.

20. Select 7. Save changes.

Setting Up NIS and NIS+

Note: Once NIS is set up, periodically inspect the server to see if the master files have changed. When a file changes, it is copied from the NIS server to the local file. The Enable field allows you to disable NIS updates without losing the setup information, so it still exists when you re-enable it.

To enable NIS or NIS+:

1. From the Configuration menu, select NIS & NIS+.

2. Select 1. Edit fields.

3. Select Y. Yes to enable the Sun StorageTek 5320 NAS Appliance to periodically update its hosts, users, and groups files through an NIS server.

4. Enter the NIS domain name, then press Enter.

5. Enter the NIS server name or IP address, then press Enter.

6. Select Y. Yes to update the hosts file through the NIS server.

7. Select Y. Yes to update the users file through the NIS server.

8. Select Y. Yes to update the groups file through the NIS server.

9. Select Y. Yes to update the netgroups file through the NIS server.
10. Enter the desired number of minutes between NIS updates, between 0 and 9, then press Enter.
11. Select Y. Yes to enable NIS+ for the Sun StorageTek 5320 NAS Appliance.
12. Enter the NIS+ home domain server address, then press Enter.
13. Enter the NIS+ home domain name, then press Enter.
14. Enter the secure RPC password for the NIS+ server. Press Enter.
15. Enter the search path as a list of domains, separated by colons. Leave this space empty to search only the home domain and its parents. Press Enter.
16. Select 7. Save changes.

Setting Name Service Lookup Order

You can choose which service is used first for user, group, and host lookup functions.

To set up lookup orders:

1. From the Configuration menu, select Lookup orders.
2. Select 1. Edit fields.
3. Select the order for resolving user information (between NIS and NIS+), then press Enter.
4. Select the order for resolving group information (between NIS and NIS+), then press Enter.
5. Select the first, second, third, and last services for resolving host information, then press Enter.
6. Select 7. Save changes.

Managing the Server File System

There are several procedures available through the console that let you manage the Server File System (SFS) volumes. The most common are described in the following sections:

Configuring Drive Letters

Drive letters are automatically assigned to file volumes available for sharing through SMB/CIFS. You can manually assign the drive letter mappings through the console, except for drive `C:`, which can only be assigned to `\cvol`.

It is possible to run out of drive letters, after which you may see the following log message:

```
No drive letter available
```

This message is for informational purposes only. The file system will be created but, to assign it a drive letter, you must reassign a drive letter that is currently used by another file system.

To manually reassign a drive letter to a file volume:

1. From the Configuration menu, select Drive Letters.
2. Enter the drive letter you want to change, then press Enter.
3. Enter the file volume name you want to assign to the new drive letter, then press Enter.

   You can only assign existing file volumes to drive letters.
4. Press Esc to exit this screen.

Creating a New Disk Volume

To create a new disk volume:

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to configure.
3. Select 1. Edit.
4. Select 1. Create partition.
5. Select the partition type for the drive.

   Press Enter to accept the default, for example, `sfs2` (primary volume) or `sfs2ext` (segment).
6. Enter the disk volume label, then press Enter.
7. If the system asks whether you want to enable Compliance Archiving on this volume and you have a license for the Compliance Archiving Software, press Y to create a compliance-enabled volume.

   Note: Sun StorageTek 5320 NAS Gateway System configurations support advisory compliance but not mandatory compliance.

   Caution: Once you enable mandatory compliance archiving on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled or downgraded to advisory.
8. Press Enter to select the default size, or enter the disk volume size in MB and press Enter.
9. Select 7. Proceed with create.

   Wait for the messages: `Initialization OK` and `Mount OK`, then press Esc to return to the Configure Disk menu.
10. When finished, press Esc until you are back to the main menu.

Renaming a Partition

If you attempt to rename a volume during a write operation, CIFS and NFS clients behave differently. If you attempt to rename a Windows volume during a write operation, CIFS I/O will stop after the volume is renamed. For NFS shares, I/O will continue after you rename a UNIX volume.

To rename a partition:

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to rename.
3. Select 1. Edit.
4. Select 3. Rename.
5. Enter the new name of the partition and press Enter.

   Note: Strict compliance-enabled volumes cannot be renamed.

Adding an Extension Segment

To add an extension, you must first create an `sfs2ext` partition on that volume.

Note: Once the extension volume is attached to the `sfs` file volume, it cannot be detached. This is an irreversible operation. The only way to separate them is to delete the `sfs` file volume.

To add an extension:

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to configure.

   Note: If you have more than 26 disk drives (disk volumes), press the spacebar to scan through them.
3. Type the number next to the partition you are changing.
4. Select 5. Segments.
5. Select 1. Add an extension segment.
6. Select the letter next to the extension drive you want.

7. Select 7. Proceed.

Deleting a Disk Volume

Note: Strict compliance-enabled volumes cannot be deleted.

Caution: All data in the volume is lost when you delete a volume.

To delete a disk volume:

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to configure.

   Note: If you have more than 26 disk drives (disk volumes), press the spacebar to scan through them.
3. Select 1. Edit.
4. Select 8. Delete.
5. Enter the disk volume name and press Enter.
6. Select 7. Proceed with delete. Wait for the messages: "`Delete OK`" and "`Delpart OK`".
7. Press Esc to return to the Configure Disk menu.
8. Press Esc until you are back to the main menu.

Shares and Quotas

You can manage shares and quotas using the console.

SMB/CIFS Shares

CIFS is a Windows file-sharing service that uses the SMB protocol. CIFS provides a mechanism for Windows client systems to access files on the Sun StorageTek 5320 NAS Appliance.

Setting Up SMB/CIFS Shares

To set up shares:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select A. Domain Configuration.
3. Enter a workgroup or domain name in the Domain field.
4. Define the domain scope, if applicable.
5. Enter a text description of the Sun StorageTek 5320 NAS Appliance server.
6. Enter the IP address of the primary and secondary Windows Internet Naming Service (WINS) servers, if applicable.
7. Assign a Keep Alive parameter.

   This is the number of seconds after which the system drops inactive connections.
8. Assign a Security Mode from Secure Share Level and NT Domain Auto UID.
9. If you are using NT Domain Auto UID mode, enter the administrative user name and password.
10. Select 7. Save changes.

    If you changed the security mode between Secure Share Level and NT Domain Auto UID, the Sun StorageTek 5320 NAS Appliance reboots.

Setting up SMB/CIFS Autohome Shares

Autohome shares are temporary shares created when a user logs on to the system and removed when the user logs off.

The autohome share feature requires two configuration parameters: state and autohome path, defined as follows:

- The state parameter defines whether the feature is enabled or disabled. The environment variable smb.autohome.enable holds the current state of the feature; the value must be yes or no.
- The autohome path parameter defines the base directory path for the temporary shares. It is defined by the `smb.autohome.path` environment variable. For example, if a user's home directory is `/vol1/home/john`, then the autohome path should be set to `/vol1/home`. The temporary share will be named `john`. The user's home directory name must be the same as the user's logon name.

If the feature is disabled, the autohome path parameter is not relevant and will not be validated.

If the feature is enabled and the path is a zero length string, the configuration will be ignored. Otherwise, the path will be validated. If the autohome path parameter does not represent an existing directory path, an informational message will be written to the system log. For example, if the specified base path was `/vol1/home`, the log message would be as follows:

```
SMB autohome: /vol1/home: no such directory
```

The log message is intended to inform the system administrator of the situation, but the configuration is still considered valid. The system will operate normally, but autohome shares will not be created. If the directory path is created at some later time, autohome shares will be added and removed, as required, from that point on.

To enable autohome shares:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select F. Autohome Setup.
3. Select 1. Edit fields.
4. Select Y. Yes to enable autohome shares.
5. Enter the autohome path.

   The autohome path defines the base directory path for the shares. For example, if a user's home directory is `/usr/home/john`, then set the autohome path parameter to `/usr/home`. The temporary share is named `john`. The system assumes that the user's home directory name is the same as the user's logon name.
6. Select 7. Save changes.

Adding a Share

After the SMB/CIFS set up is complete, you must define SMB/CIFS shares. Shares allow Windows users to access directories in the Sun StorageTek 5320 NAS Appliance.

To add a share:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.
3. Select 8. Add a share.
4. Enter a share name.
5. Enter a path in the directory, in the form volume/directory.

6. Enter a comment about this directory, if applicable.
7. If your system is configured for Workgroup mode:
   - In the Password Protection pull-down menu, select Yes or No.

     If enabled, there is an option for either read/write or read-only.
   - Enter User ID, Group ID, and Umask.
8. Select 7. Save changes.

Editing a Share

To edit a share:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.
3. Enter the letter corresponding to the share you are editing.
4. Select 1. Edit fields.
5. Enter the new share name, directory, comment, password information, user ID, and group ID.
6. If your system is configured for Workgroup mode:
   - In the Password Protection pull-down menu, select Yes or No.

     If enabled, there is an option for either read/write or read-only.
   - Enter User ID, Group ID, and Umask.
7. Select 7. Save changes.

Deleting a Share

To delete a share:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.
3. Enter the letter corresponding to the share you are deleting.
4. Select 8. Delete.

Setting Up Active Directory Service

When the Active Directory Service (ADS) is enabled and set up, the Sun StorageTek 5320 NAS Appliance automatically performs ADS updates.

To enable ADS service:

1. From the Extensions menu, select ADS Setup.
2. Select 1. Edit fields.
3. Select Y. Yes to let the ADS client publish Sun StorageTek 5320 NAS Appliance shares to ADS.
4. Enter the Windows domain on which ADS is running.

   The Sun StorageTek 5320 NAS Appliance must also belong to this domain.
5. Enter the name of a Windows user with administrative rights.

   The ADS client verifies secure ADS updates with this user.
6. Enter the Windows administrative user's password.
7. In the User Container field, enter the ADS path for the Windows administrative user in LDAP DN notation.

   For more information see "Enabling ADS" on page 77.
8. If the ADS domain uses sites, enter the appropriate site name in the Site field. Otherwise, leave the Site field blank. If specified, the Site will be included when selecting a domain controller.
9. Enter, in uppercase letters, the Kerberos realm name used to identify ADS.

   This is normally the ADS domain
10. Enter the host name of the Kerberos Key Distribution Center (KDC) server.

    This is usually the host name of the main domain controller in the ADS domain. You can leave this field blank if the ADS client or dynamic DNS client can locate the KDC server through DNS.
11. Select 7. Save changes.

Enabling and Disabling Quotas

Quotas track and limit the amount of disk space each user and group uses. You can turn the quota tracking function on and off. This function only enables and disables quotas. It does not set quota limits.

Note: Quota initialization takes several minutes, during which time the volume is locked and unavailable to users.

To enable or disable quotas:

1. From the Configuration menu, select Disks & Volumes.
2. Select the drive for which you are enabling quotas.
3. Select 1. Edit.
4. Select 4. Quotas on/off.
5. Select 1. Turn quotas on or 8. Turn quotas off.

Security

You can set up groups and credential mapping to ensure security. The tasks are described in the following sections:

Configuring User Groups

The requirements for built-in local groups are different from those of a Windows NT system. For a complete description of user groups, see "About Local Groups" on page 84.

Adding a Group

To add a group:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press 8. Add a Group to add a local group.
4. Type in the name of the group and press Enter.
5. Type in a description of the group, if applicable, and press Enter.
6. Press 7. Save Changes to save the new group.

Adding a Member to a Group

To add a member to a group:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press the letter of the group you want to modify.
4. Press 2. Members to change the membership of the group.
5. Press 8. Add to add a member.
6. Type in the domain and user name in the following format: *domain**username*

   The domain identifies the domain where the user name can be authenticated. For example, typing `BENCHLAB\john` identifies the domain `BENCHLAB` where the user `john` can be authenticated.
7. Press Enter.
8. Press 7. Save Changes to save the new member.

Removing a Member From a Group

To remove a member from a group:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press the letter of the group you want to modify.
4. Press 2. Members to change the membership of the group.
5. Press the letter corresponding to the group member you want to remove.
6. Press Y in response to the prompt.

Modifying Group Privileges

A description of the user group privileges is provided in "About Configuring Privileges for Local Groups" on page 84.

To modify local group privileges:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press the letter of the group you want to modify.
4. Press 3. Privileges to change the privileges of the group members.
5. Press the letter of the privilege that you want to add or remove.
6. Press 7. Save Changes to save the changes that you made.

User and Group Maps

For a complete description of user and group credentials, see "About Mapping User and Group Credentials" on page 92.

Adding a User Map

To add a user map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select C. User Mapping.
3. Press 8. Add a map.
4. In the Account field, enter the domain and name of the NT user that you want to map to a UNIX user.

   Use the format *domain\username*.
5. In the Name field, enter the name of the UNIX user that you want to map to the NT user.
6. Press 7. Save Changes.

Editing a User Map

To edit a user map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select C. User Mapping.
3. Press the letter of the map that you want to edit.
4. Press 1. Edit Fields.
5. Type your changes and press Enter.
6. Press 7. Save Changes.

Removing a User Map

To remove a user map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select C. User Mapping.
3. Press the letter of the user map that you want to delete.
4. Press 8. Delete.

Adding a Group Map

To add a group map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press 8. Add a map.
4. In the Account field, enter the domain and name of the NT group that you want to map to a UNIX group. Use the format *domain\username*.
5. In the Name field, enter the name of the UNIX group that you want to map to the NT group.
6. Press 7. Save Changes.

Editing a Group Map

To edit a group map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press the letter of the group map that you want to edit.
4. Press 1. Edit Fields.
5. Type your changes and press Enter.
6. Press 7. Save Changes.

Removing a Group Map

To remove a group map:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press the letter of the group map that you want to delete.
4. Press 8. Delete.

Mapping and Securable Objects

This section details the interaction between user or group credential mapping and the securable objects within the system, for example, files and directories in the file system.

Objects residing on the system are classified according to the domain from which its security attributes were set. Objects that are created using the NFS Protocol have only UNIX security attributes and thus are classified as UNIX objects. Objects created using the SMB Protocol have both UNIX and Windows security attributes; they are classified as Windows objects. Although it is possible to allow objects to migrate from either domain to the other, as the security attributes are changed, a policy decision has been made that only one of the migrations will be allowed. A UNIX object becomes a Windows object when its security attributes are changed using SMB. By default, the security attributes of a Windows object cannot be changed using NFS. This is because Windows security is based on security descriptors, which cannot always be accurately represented using UNIX security attributes. Allowing a Windows object to become a UNIX object could potentially weaken the access control protecting the object.

Two mechanisms are provided to allow the attributes of a Windows object to be modified via NFS: the `chsmb` command and the `acl.overwrite.allowed` environment variable.

If the `acl.overwrite.allowed` is not present or is set to "no," the default volumebehavior will be applied; that is, the attributes of a Windows object cannot be changed via NFS.

If the `acl.overwrite.allowed` environment variable is set to "yes," UNIX commands, such as `chown`, `chgrp`, and `chmod` will be permitted, according to the standard UNIX access rules. If the attributes of a Windows object are modified using NFS, the Windows security descriptor will be deleted, and the object will become a UNIX object.

The `chsmb` command can be used to remove a single Windows security descriptor or the entire Windows security descriptor database for a volume. To apply the `chsmb` command to an individual file or directory, you must specify the absolute path to that object. Note that `chsmb` does not preform recursive operations, so subdirectories or files contained within a directory will not be affected if the command is applied to a directory. The following examples illustrate how to use the `chsmb` command.

To delete the security descriptor and revert to the UNIX permissions on `/vol1/shared/bin/file.doc`, use the following command:

```
chsmb /vol1/shared/bin/file.doc
```

To delete all security descriptors on `/vol1` and revert all files to their UNIX permissions, use the following command:

```
chsmb /vol1
```

The `chsmb` command affects file security, so extra care should be taken when using this command. When a volume is specified, the `chsmb` command will issue a warning and prompt for confirmation before any action is taken.

No mapping is performed when a Windows user accesses a Windows object. Similarly, no mapping is performed when a UNIX user accesses a UNIX object. These are considered to be native access conditions. Also, because Windows objects have both Windows and UNIX security attributes, no mapping is required when a UNIX user accesses a Windows object, even though it is a nonnative access situation. This is a direct benefit of the design decision to choose one of the domains as the default mapping rather than creating an independent neutral mapping. Thus the only time that mapping is required is when a Windows user accesses a UNIX object. When a Windows user accesses a UNIX object, the object's UNIX security attributes are mapped to the Windows domain and the Windows security policy is applied.

Configuring the Host List

The console allows you to configure host information.

Adding a Host

To add a host:

1. From the Configuration menu, select Hosts.
2. Type the new host name, then press Enter.

   The system verifies that the host name does not already exist.
3. Press Enter to add the host.
4. Enter the new host IP address.
5. Select 7. Save changes.

Editing an Existing Host

To edit an existing host:

1. From the Configuration menu, select Hosts.
2. Type the name of the host you are editing and press Enter.
3. Select 1. Edit.
4. Enter the new host name or IP address.
5. Select 7. Save changes.

Deleting a Host

To delete a host:

1. From the Configuration menu, select Hosts.
2. Type the name of the host you are deleting and press Enter.
3. Select 8. Delete.

Managing Trusted Hosts

Use the Trusted Hosts menu option to manage hosts that have unrestricted access to all resources.

Designating a Trusted Host

To designate a trusted host:

1. From the Access Control menu, select Trusted Hosts.
2. Type a host name, then press Enter.

   Note: To add a trusted host, the host must exist on the host list or NIS.

   The system verifies that the trusted host name does not already exist. If the trusted host exists, the host information is displayed. If the host is not trusted, the system displays a warning.

3. Select 7. Add to list.

   The new trusted host is added, and the system displays the name at the top of the screen.

Deleting a Trusted Host

To delete a trusted host:

1. From the Access Control menu, select Trusted Hosts.
2. Type in the name of the trusted host you are deleting and press Enter.
3. Select 8. Delete.

   The trusted host is removed from the list.

Managing Volume Access

Once you save the changes, the existing NFS mounts from clients are updated to reflect the new parameters.

Do not allow any access, either read or write, to the `cvol` volume.

Note: Trusted hosts are automatically granted read/write access to file volumes regardless of the volumes' access settings.

Managing Volume Access for NFS Clients

To manage volume access for NFS clients:

1. From the Access Control menu, select Volume Access.
2. Enter the letter corresponding to the volume to change its access.
3. Enter the number corresponding to the type of access you are assigning; read/write access, read-only access, or no access.

   Note: Hosts on the trusted list are allowed read/write access regardless of the volume access parameters.

4. Select 7. Save changes.

Locking and Unlocking the Console

You can use the console to disable or enable most of the main menu options, preventing unauthorized use of the console. You must set the administrative password to secure the console.

Locking the Console

To lock the console:

1. From the Operations menu, select Lock Console.
2. Enter the administrative password.
3. Select Y (Yes).

Unlocking the Console

To unlock the console:

1. From the main menu, select Unlock Console.
2. Enter the administrative password.
3. Select Y (Yes).

Mirroring File Volumes

This section describes how to mirror file volumes from a Sun StorageTek 5320 NAS Appliance active system to a Sun StorageTek 5320 NAS Appliance mirror system. For more information on mirroring, see Chapter 9.

Note: When using file replication on a Sun StorageTek 5320 NAS Cluster Appliance, do not perform mirror operations, such as change role, when the Cluster is in a degraded state.

Configuring Active and Mirror Servers

After the primary IP addresses have been configured on the active and mirror servers and you have designated the roles of the ports connecting the Sun StorageTek 5320 NAS Appliance mirror servers to one another, you can configure mirroring on the active and mirror servers using the console interface.

Configuring a New Active Server With a New Mirror Server

Follow these steps first on the active server and then, using Telnet, on the mirror server.

To configure a new active server with a new mirror server

1. From the Configuration menu, select Host Names and Network.
2. Select 1. Edit Fields.
3. If you have not done so already, configure the ports connected to a local network or subnet.

   For more information about configuring TCP/IP using the console, see "Configuring TCP/IP" on page 221. For more information on configuring ports, see Chapter 5.
4. Assign the server name and IP address for the port used for the connection between the active and mirror systems.
5. In the Role field of the port used for the connection between the active and mirror servers, select mirror.
6. Select Save to save changes and return to the main menu.
7. Set up DNS and NIS/NIS+, if these services are available, and the name service lookup order.

   For more information about setting up name services, see "Name Services" on page 227.

   The network connections of the active and mirror systems are now configured. See the following section to continue.

Configuring an Existing Active Server With a New Mirror Server

To configure an existing active server with a new mirror server:

1. On the active server, in the Configuration menu, select Host Names and Network.
2. Select 1. Edit Fields.
3. Assign the server name and IP address for the port used for the connection between the active and mirror systems.
4. In the Role field of the port used for the connection between the active and mirror servers, select mirror.
5. Open a Telnet window to the mirror system, and repeat steps 1. - 4..
6. In the Telnet window of the active server, press Esc until you reach the following command line:

   ```
   connect to (? for list) ? [menu]
   ```

7. Log in as the administrator.
8. Enter the following:

   `ping` ***`xxx.xxx.xx.xx`***

   where *xxx.xxx.xx.xx* is the IP address of the mirror server.

9. On the mirror server, log in as administrator and enter the IP address of the active server.

   The network connections of the active and mirror systems are now configured. Continue by configuring file volumes for mirroring.

Configuring File Volumes

Mirroring is performed on a per-volume basis. You can mirror some or all of your volumes.

Note: Once you mirror a file volume, you cannot rename the file volume while maintaining the mirroring connection. You can only mirror file volumes equal to or larger than 1 gigabyte.

Setting Up a File Volume for Mirroring

To set up a file volume for mirroring:

1. On the active system, create a small (for example, 32-MB) file volume named SYS before creating any other volumes.

   If you already have file volumes on the active system, this step is optional.

2. On the active system, in the Configuration menu, select Disks and Volumes.
3. Select the drive on which you want to create the new file volume.
4. Select Create & init partition. Then select 1. sfs2.
5. Enter SYS for the name, and 64 for the size in MB.

   This forces residence of the `/etc` directory and the Sun StorageTek 5320 NAS Appliance configuration files it contains on the SYS volume.

6. Repeat steps 1.- 5.on the mirror system.

   Do not create any other file volumes on the mirror system.

Mirroring File Volumes

To mirror file volumes:

1. Using Telnet, connect to the active system and enter the main menu.
2. In the Operations menu, select Licenses and select the letter corresponding to Mirroring.
3. Enter the activation key exactly as provided by Sun Microsystems.
4. Press Esc until you see the main menu.
5. In the Extensions menu, select Mirrors.
6. Select Add mirror to create a new mirror.
7. Select a file volume to be mirrored by pressing the corresponding letter.

   The file volume must be equal to or larger than 1 GB.

8. Enter the host name of the mirror system.
9. Enter the private IP address, if necessary.

   This is the IP address used for the mirroring connection with the mirror server.

10. Enter the alternative IP addresses in the Alt IP Address fields.

11. If accessing the mirror server requires an administrative password, enter it in the Remote admin password field.
12. Enter the size of the Transaction Buffer Reserve, then press Enter.
13. Select 7. Proceed to add the mirrored file volume.

    When the mirror volume reaches an in sync state (with the active volume), the mirror volume is mounted as read-only.

    Note: There can be no I/O activity to the active server during initial mirror synchronization.

    During and after the mirror creation process, the system displays the Mirror Creation screen.
14. To view the status of the mirror, select A.
15. To edit the alternate IP addresses or administrator password, select 1. Edit.

Setting Warning Thresholds

When the transaction buffer reserve fills and overruns, the mirror is cracked. This screen allows you to set the percentages at which warnings are issued. The default percentages are 70, 80, and 90 percent.

To set the threshold percentages at which warnings are issued:

1. On the active system, in the Extensions menu, select Mirrors.
2. Select 3. Threshold Config.
3. Select 1. Edit to edit the percentages shown on this screen.
4. Enter the desired percentages.
5. Enter the number of hours the system should wait before reissuing the same threshold warning in the Alert Silent Period field.
6. Select 7. Proceed.

Promoting a Mirrored File Volume

In the event that the active system fails, the mirror system provides high availability. To make a mirrored file volume available to network users, promote the file volume. You must first break the mirror by disconnecting the active-mirror connection between the active file volume and the mirrored file volume. Then promote the volume and configure the mirrored file volume access rights. Once you break the mirror and promote the mirrored file volume, the two file volumes are completely independent.

To promote a file volume on the mirror system:

1. On the mirror system, view the status of the file volume by selecting Disks & Volumes from the Configuration menu.

   The "*" (asterisk) appearing after the name of the mirrored file volume indicates that the file volume is currently mirrored.

   You should only break the mirrored file volume from the mirror system if the active system is down. To promote a file volume when the active system is up, break the mirror from the active system (not the mirror system).

2. In the Extensions menu, select Mirrors.
3. Select the letter corresponding to the mirrored file volume that you are breaking.
4. Select 8. Break.

   Note: If possible, break the mirror from the active system.

5. When prompted to confirm the break, select Y. Yes to continue.
6. Press Esc to return to the main Mirrors screen.
7. In the Extensions menu, select Mirrors.
8. Select 1. Promote Volume.
9. Select the letter corresponding to the file volume that you want to promote.
10. Select 7. Proceed to promote the file volume.

    It might take several minutes to complete this process. For a mirrored file volume to be promoted, it must have reached an In Sync state at least once.

11. When the system finishes promoting the file volume, press Esc to return to the main menu.
12. (Optional) To configure NFS file volume access, select Volume Access from the Access Control menu.

13. Set the access rights to the file volume by selecting its corresponding letter.

14. Choose Read/write, Read only, or None.

15. Select 7. Save changes to continue.

    The volume has been promoted. To reestablish a mirror, see the following section, "Reestablishing a Mirror" on page 254.

Reestablishing a Mirror

This procedure describes how to reestablish a mirror when the active server has failed and you have promoted the file volume on the mirror server. The promoted file volume is now the most up-to-date version and functions completely independently of the out-of-date file volume on the active system. To recreate the mirror, mirror the up-to-date file volume back to the active server and then mirror the file volume back to the mirror server as it was originally.

If you have not promoted the mirrored file volume, do not follow these instructions. The active system automatically brings the mirror back to an In Sync state when it is back online.

In the examples that follow, Server 1 is the active server and Server 2 is the mirror server.

Reestablishing a mirror includes the following steps:
- Breaking the mirror on Server 1
- Deleting the out-of-date file volume on Server 1
- Mirroring the up-to-date file volume from Server 2 back to Server 1
- Change roles, making Server 1 active again and Server 2 the mirror server

When the active server is brought online, it might attempt to reestablish the mirror. Therefore, you must break the mirror on Server 1.

Breaking the Mirror on Server 1

To break the mirror on Server 1:

1. On Server 1, in the Extensions menu, select Mirrors.

2. Select the letter corresponding to the mirrored file volume.

3. Select 8. Break.

4. Select Y. Yes to confirm breaking the mirror.

Deleting the Out-of-Date File Volume on Server 1

To delete the out-of-date file volume on Server 1:

1. Press Esc to return to the main menu.
2. In the Configuration menu, select Disks & Volumes.
3. Select the number corresponding to the mirrored file volume.

Caution: Before completing the following step, be sure you are deleting the out-of-date file volume on Server 1. Also, be sure that the up-to-date file volume on Server 2 is verified and promoted first.

4. Select 8. Delete.
5. Enter the file name of the out-of-date file volume.
6. Select 7. Proceed with delete to delete the out-of-date file volume.

Mirroring the Up-to-Date File Volume on Server 2 Back to Server 1

To mirror the up-to-date file volume on Server 2 back to Server 1:

1. On Server 2, in the Extensions menu, select Mirrors.
2. Select 8. Add mirror.
3. Select the letter corresponding to the file volume that you are mirroring.
4. Enter the private host name of Server 1.
5. Enter the private IP address, if necessary, and the administrator password.
6. Enter the transaction buffer reserve.

   For more information, see "Mirroring File Volumes" on page 251.
7. Select 7. Proceed.
8. During the mirror creation process, select the letter corresponding to the new mirrored file volume.

   When the mirror reaches an In Sync state, an identical copy of the file volume exists on both Server 1 and Server 2.

   Youa re now ready to change roles. See "Changing Roles" on page 256.

Changing Roles

To change roles:

1. From the main menu select the Mirror option on Server 1.
2. Select desired volume by pressing the appropriate letter.
3. For example, press “A” to select the “cvol1” file volume.
4. From the Mirror Status menu, select the Change Role option.

   Note: Make sure the volumes are 100 percent in sync before changing roles.
5. Select Yes to confirm.

Monitoring

You can use the console to perform monitoring functions. The following sections describe how to set up and access monitoring functions:

- "Configuring SNMP" on page 256
- "Configuring Email Notification" on page 257
- "Viewing System Information" on page 257

Configuring SNMP

The SNMP menu lets you send messages to a remote SNMP monitor, as well as modify the community string, contact information, and the location of the SNMP monitor.

To configure SNMP:

1. From the Extensions menu, select SNMP Configuration.

   Public is the default Community name. You can enter any name you want.
2. Select 1-5. Edit a Trap Destination to add, edit, or delete a trap destination, 6. Edit Community to edit the community string, 7. Edit Contact to edit contact information, or 8. Edit Location to edit the location of the remote SNMP monitor.
3. Select Y. Yes to save your changes.

Configuring Email Notification

When there is a problem with your system, Sun StorageTek 5320 NAS Appliance sends email messages to specific recipients.

Note: You must configure DNS for email notification to function properly.

To configure email notification:

1. From the Extensions menu, select EMAIL Configuration.
2. Select 1. Edit fields.
3. Type the information requested for each field. Press Enter to move between fields.
   - **SMTP Server** – This is the mail server; all mail is directed here. The host file or the DOS server must include the server name.

     Note: You can use the IP address or the name. The name must be resolved by your DNS server.
   - **Recipient 1–4** – These are the email addresses of the four people automatically notified in case of a problem.
   - **Notification Level** – The level a problem must be at before the recipients are notified through email. Select one of the following:

     Errors – Notifications sent only for errors

     Errors and warnings – Notifications sent for errors and low priority warnings

     None – No notifications sent
4. Select 7. Save Changes to save the current configuration.
5. Press Esc to return to the main menu.

Viewing System Information

You can view system information from the console.

Viewing Server Status

To view server status:

1. From the Operations menu, choose Activity Monitor.

   The Activity Monitor screen lists the following information:

   - **Volume** – Displays the first 22 file volumes.
   - **Use%** – Displays the amount of space used on the volume.
   - **Reqs** – Displays the number of requests processed for the volume in the last 10 seconds.
   - **Device** – Displays the name of the device.
   - **Load** – Displays the percentage of CPU load.
   - **Peak** – Displays the highest usage per second in the last 10 minutes.
   - **Client** – Displays name or address of the user.
   - **Reqs** – Displays the number of requests processed for the volume in the last 10 seconds.

2. Press Esc to return to the main menu.

Viewing the System Log

- **To view the system log, rom the Operations menu, select Show Log.**

The log displays two types of entries:

- **System Startup Log Entries** – Reports device configurations, volumes, and other pertinent information
- **Normal Operation Log Entries** – Reports device errors, security violations, and other routing status information. The release number and software serial number are listed last.

Viewing Port Bonding

To view port bonding:

1. From the Configuration menu, select Host Name & Network.
2. Press the spacebar to scroll to the next panel.

   The bond1 column shows the first port bond. The input/output information in this column is the sum of the input/output information in the two ports that you bonded.

Viewing the Checkpoint Analysis

To view the checkpoint analysis:

1. From the Configuration menu, select Disks & Volumes.
2. Type the letter corresponding to the drive that you are configuring.
3. Select Change/Delete volume name.
4. Select 6. Checkpoints.
5. Select 3. Analysis. Scroll through the analysis using the spacebar.
6. Select 0. End Analysis to exit this screen.

Viewing the Status of a Mirrored File Volume

To view the status of a mirrored file volume:

1. On the active system, select Mirrors from the Extensions menu.
2. Select the mirrored file volume.

   There are three sections of the status screen:

   - The first line displays the mirror state information, including file volume name, mirror state, a progress indicator, and a status message. There are ten mirror states:
     - ERR – An error has occurred.
     - NEW – A new mirror is being created.
     - INIT – The mirror buffer is being initialized.
     - MKPT – Disk partitions are being created on the mirror system.
     - RDY – The system is ready and waiting for the other system to be ready.
     - DOWN – The network link is down.
     - CRK – The mirror is cracked.
     - RPL – The replication phase is occurring.
     - OOS – The mirror is out of sync.
     - SYNC – The mirror is in sync.

     The progress indicator displays a progress percentage of activity within each state. A status message also gives a short text message describing the mirror status.
   - The second line displays the condition of the transaction buffer reserve. The information displayed here is the maximum number of transactions the buffer can hold, the next transaction id, the sync transaction id, the head transaction id, and an In Sync percentage indicator describing the state of synchronization between the active and mirror systems.

On the active system:

- The next xid (next transaction id) identifies the next transaction id of the file system.
- The sync xid (sync transaction id) identifies the last transaction that was transferred to the mirror system.
- The head xid (head transaction id) identifies the last transaction that was acknowledged by the mirror system.
- When the In Sync percentage indicator is 100 percent, the mirror system has a complete copy of the active system. If the In Sync percentage indicator displays 0 percent, then the mirror is cracked and the active server automatically performs a block by block resync. While the mirror state is in the Out Of Sync state, the mirror volume is volatile until the mirror is back in sync.

On the mirror system:

- The next xid (next transaction id) identifies the next transaction that is expected from the active system.
- The sync xid (sync transaction id) identifies the last transaction that was scheduled to be written to disk.
- The head xid (head transaction id) identifies the last transaction that was acknowledged on disk.
- When the In Sync percentage indicator is 100 percent, all mirror transactions have been written to disk, and the mirror system volume is an exact copy of the active system volume.

3. To edit the alternate IP addresses or administrator password, select 1. Edit.
4. Edit the fields, then select 7. Proceed to save your changes.
5. To see network statistics on the mirrored file volume, select 2. Statistics.

   The screen displays the statistics for the active system, including the number of transactions into the active file volume (IN) and out of the active system to the mirrored file volume (OUT). The screen shows the average, minimum, and maximum transactions per second (t/s) for each.

   The system displays the amount of free space remaining in the transaction buffer reserve (Buffer), along with the fill rate. If the fill rate is greater than zero, you should check to make sure that all network links are functioning properly. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. When the buffer overruns, the mirror is cracked.

Viewing Network Statistics for All Mirrored File Volumes

To view network statistics for all mirrored file volumes:

1. On the active system, select Mirrors from the Extensions menu.
2. Select 2. Network Statistics.

   The screen displays the total number of RCBs (Request Control Blocks) sent, the number of RCBs sent per second, and the average size of the RCBs, as well as their average response time and transfer rate.
3. Select 1. Reset to restart this display.

System Maintenance

There are several system maintenance and setup functions that can only be performed from the console. These include the following:

- "Configuring File Transfer Protocol (FTP) Access" on page 262
- "Managing RAID Controllers" on page 263
- "Mounting File Systems" on page 265

Additional tasks can be performed from the console administrator as well as from the Web Administrator:

- "Shutting Down the System" on page 265
- "Managing LUN Failover" on page 265
- "Configuring LUN Paths" on page 267
- "Scheduling File Checkpoints" on page 268
- "Configuring NDMP Backup" on page 268
- "Configuring the Compliance Archiving Software" on page 269
- "Configuring System Auditing" on page 270

Configuring File Transfer Protocol (FTP) Access

FTP is an Internet protocol used to copy files between a client and a server. FTP requires that each client requesting access to the server must be identified with a username and password.

Types of Users

You can set up three types of users:

- **Administrators** who have the user name `admin` and use the same password used by GUI clients.

  The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as "/".

- **Users** who have a user name and a password specified in the local password file or on a remote NIS or NIS+ name server.

  The user has access to all existing directories and files within the user's home directory. The home directory is defined as part of the user's account information and is retrieved by the name service.

- **Guests** who log in with the user name `ftp` or its alias `anonymous`. A password is required but not authenticated. All guest users have access to all directories and files within the home directory of the `ftp` user.

  Note: Guest users cannot rename, overwrite, or delete files; cannot create or remove directories; and cannot change permissions of existing files or directories.

Setting Up FTP Access

To set up FTP access:

1. From the Extensions menu, select FTP Configuration.
2. Select 1. Edit Fields.
3. Select Y. Yes to enable FTP or N. No to disable it.

   If FTP service is enabled, the FTP server will accept incoming connection requests.

4. In Allow guest access, select Yes to enable access to the FTP server by anonymous users or No to disable access.
5. In Allow user access, select Yes to enable access to the FTP server by all users or No to disable access.

   This does not include the `admin` or root user.

   Note: User names and passwords must be specified in the local password file or on a remote NIS or NIS+ name server.
6. In Allow admin access, select Yes to enable root access to those in possession of the Sun StorageTek 5320 NAS Appliance administrative password (use with caution) or No to disable access.

   Note: A “root” user is a user with UID equal to 0 and the special Sun StorageTek 5320 NAS Appliance user “admin”.
7. In Enable logging, select Yes to enable logging or No to disable logging.
8. If you enable logging, in Log filename specify the log file name.
9. Select 7. Save changes.

Managing RAID Controllers

The `raidctl` command enables you to manage RAID controllers from the CLI.

For all `raidctl` commands, follow instructions for "Accessing the Console Administrator Command-Line Interface" on page 218.

Caution: Use commands carefully to avoid unintended results.

Getting Help on Subcommands

To get help on subcommands, at the command line, enter **`raidctl help`**.

Controlling LEDs

To control LEDs:

1. To cause all LEDs in a tray to blink, enter:

   **`raidctl locate type=lsi target=tray ctlr=0..`*`n`*` tray=0..`*`n`*

2. To cause a specified drive's LED to blink, enter:

   raidctl locate type=lsi target=drive ctlr=0..*n* tray=0..*n* slot=1..*n*

3. To stop blinking LEDs for a specified controller, enter:

   raidctl locate type=lsi action=stop ctlr=0..*n*

Getting Events and Configuration Information

To get events and configuration information:

1. To get all events for a specified controller, enter:

   raidctl get type=lsi target=events ctlr=0..*n*

   The log of all events will be written to `/cvol/log/2882ae.log` file. If the file already exists, you will be prompted to overwrite the file, specify a new file name, or cancel the operation.

2. To get critical events for a specified controller, enter:

   raidctl get type=lsi target=events ctlr=0..*n* etype=critical

   The log of critical events will be written to `/cvol/log/2882ce.log` file. If the file already exists, you will be prompted to overwrite the file, specify a new file name, or cancel the operation.

3. To get configuration information for a specified controller, enter:

   raidctl get type=lsi target=profile ctlr=0..*n*

Setting the Controller Time and Battery Age

To set the controller time and battery age:

1. To reset a specified controller's battery age, enter:

   raidctl set type=lsi target=battery-age ctlr=0..*n*

2. To synchronize a controller's time with the server's time, enter:

   raidctl set type=lsi target=ctlr_time-age ctlr=0..*n*

Downloading Firmware

To download firmware, use the **raidctl download** command.

Note: Refer to Chapter 11 for firmware upgrade procedures.

Mounting File Systems

After multiple continuous reboots, one or more file systems may become unmounted. To mount the file systems, issue the following command:

`mount -f` *volume-name*

Shutting Down the System

The Sun StorageTek 5320 NAS Appliance system is designed for continuous operation, but if you need to shut down the system, you must do it from the Web Administrator, the console, or the LCD panel.

To shut down the system:

1. From the Operations menu, select Shutdown.
2. Select the desired option by typing the appropriate letter option.
   - **R. Reboot** – Type "R" to reboot the system.
   - **H. Halt** – Type "H" to halt the system.
   - **P. Boot Previous Version 4.x.xx.xxx** – Type "P" to reboot the system using the available previous OS version. This option is available on systems that have more than one OS version installed.
   - **ESC** – Press the Esc key to cancel and return to the main menu.

   If you choose to reboot, halt, or boot with the previous OS version, the server reboots or turns off after all the delayed writes to disks are completed.

Managing LUN Failover

Failover occurs when one of the two heads becomes unreliable and all LUNs under its control must be moved to the stable head. The Failover menu manages disk resources when a recoverable error occurs.

Configuring Failover

To configure failover:

1. From the Extensions menu, select Failover/Move LUNs.

   Note: Failover/Move LUNs is available only in cluster configurations. You cannot enable or disable LUN failover for a single head system.

2. If the option is available, select 3. Edit Failover.

3. Select Y. Yes to enable head failover.

4. If you are using a Sun StorageTek 5320 NAS Cluster Appliance or a Sun StorageTek 5320 NAS Gateway System dual server in a cluster configuration:
   - Select Y. Yes to enable link failover. Link failover ensures that an alternate network link becomes active when a primary link fails.
   - Enter the number of seconds before link failover occurs, in the event that one network link becomes unreliable.
   - Enter the number of seconds before link restore occurs, in the event that the original link is repaired or reconnected.

5. If you are a Sun StorageTek 5320 NAS Cluster Appliance or Sun StorageTek 5320 NAS Gateway System cluster configuration user's select 2. Modify to rearrange LUN ownership by adapter. When the restore process occurs, this is the resulting configuration.
   - Enter the LUNs owned by each adapter.
   - Separate the numbers by a single space (for example, 0 2 8 10).
   - Press Enter.

6. Select Y. Yes to save your changes.

Restoring the System, Initiating Failback

To restore the system, initiating failback:

1. Replace or repair the faulty component and make sure that it is online.

2. From the Extensions menu, select Failover/Move LUNs.

   Note: Failover/Move LUNs is available only in cluster configurations. You cannot enable or disable LUN failover for a single head system.

3. Select 1. Restore.

4. Select Y. Yes to proceed with the restore process.

Configuring LUN Paths

See "About Setting LUN Paths" on page 15 for more information on LUN paths subject and the use of the GUI in setting them.

To edit a LUN path:

1. From the Extensions menu, press the spacebar until the LUN Ownership option is displayed and select it.

   The LUN Ownership screen displays all LUNs whose paths can be changed. A LUN can be reassigned only if there are no file systems on that LUN. On a Sun StorageTek 5320 NAS Cluster Appliance or a Sun StorageTek 5320 NAS Gateway System in a cluster configuration, only the head that “owns” a LUN can reassign it to another head.

   Note: On a Sun StorageTek 5320 NAS Cluster Appliance or a Sun StorageTek 5320 NAS Gateway System in a cluster configuration, when you first start the system, all LUNs are assigned to one head (Head 1). You must use Head 1 to reassign some LUNs to Head 2 for even distribution.

   Note: LUNs that have no LUN path assigned might initially appear multiple times in the LUN Ownership screen, as their presence is advertised by multiple controllers over multiple paths. Once a LUN has a path assigned, it is shown once, on its current path.

2. Select a LUN path by typing the letter to the left of the desired path.

3. Select 1. Edit to edit the LUN path.

   The Configure LUN Path screen displays all the available paths for the LUN. The current or active LUN path is marked as “Active”. If the primary path is set for the LUN, it is marked as "PRIMARY."

4. Type the number of the desired LUN path to which you want to change and press Enter.

   Evenly divide the assignment of LUNs to the two available paths. For example, the first and third LUN to path 1. and the second and fourth LUN to path 2.

5. Select Y. Yes to save your changes.

Scheduling File Checkpoints

A checkpoint is a virtual read-only copy of a primary file volume. See "About File Checkpoints" on page 162 for detailed information about checkpoints.

To schedule checkpoints:

1. From the Configuration menu, select Disks & Volumes.
2. Select the drive for which you are scheduling checkpoints.

   Note: If you have more than 26 drives (disk volumes), press the spacebar to scan through them.
3. Select 1. Edit.
4. Select 6. Checkpoints.
5. Follow the prompts at the bottom of the screen, pressing Enter to move through the fields.
6. When you have entered all checkpoint information, select 7. Save changes.

Configuring NDMP Backup

To back up system volumes, you must first add a backup job, then schedule or run it. Be sure the backup device is online before proceeding.

Note: Checkpoints must be enabled for volumes to be backed up by the Network Data Management Protocol (NDMP). Refer to "About File Checkpoints" on page 162.

To set up NDMP:

1. From the Extensions menu, select NDMP Setup.
2. Select the NIC port used for data transfer to the backup tape drive, and press Enter.

   All available ports are shown below this field.
3. Select a spare volume path, such as `/vol_ndmp`, of at least 2 GB for saving NDMP log and data files.

   You should use a totally separate file volume for this apart from the volumes which are scheduled for backup.

4. Save changes.

Configuring the Compliance Archiving Software

If you have purchased, activated, and enabled the Compliance Archiving Software option (see "Activating System Options" on page 121), there are additional settings you can establish using the command-line interface.

Note: Sun StorageTek 5320 NAS Gateway System configurations support advisory compliance but not mandatory compliance.

Caution: Use commands carefully to avoid unintended results.

Changing the Default Retention Period

To change the default retention period:

1. Follow instructions for "Accessing the Console Administrator Command-Line Interface" on page 218.
2. At the command line, enter **`fsctl compliance`** *volume* **`drt`** *time*

   where *volume* is the name of the volume for which you want to set the default retention time, and *time* is the duration of the default retention time in seconds.

   To set the default retention to "permanent," you should use the maximum allowable value, `2147483647`.

Enabling CIFS Compliance

In its initial configuration, the Compliance Archiving Software supports data retention requests only from NFS clients. Common internet file system (CIFS) access to this functionality can be enabled from the command-line interface.

Caution: Use commands carefully to avoid unintended results.

To allow Windows clients to use the Compliance Archiving functionality:

1. Follow instructions for "Accessing the Console Administrator Command-Line Interface" on page 218.

2. At the command line, enter **`fsctl compliance wte on`**.

Configuring System Auditing

System auditing is a service that allows the administrator to audit particular system events by storing records of those events in log files. For more details about system auditing, refer to "About System Auditing" on page 149.

To configure system auditing:

1. From the Extensions menu, select System Audit Configuration.
2. Select 1. Edit fields.
3. Enable auditing and specify the path for the audit log and the maximum file size for the log file.
4. Select 7. Save changes to save changes.

APPENDIX **B**

Sun StorageTek 5320 NAS Appliance Error Messages

This appendix describes the error messages produced by the various components of the Sun StorageTek 5320 NAS Appliance system. It includes the following sections:

About Sun StorageTek 5320 NAS Appliance Error Messages

This appendix details the specific error messages sent through email, Simple Network Management Protocol (SNMP) notification, the liquid crystal display (LCD) panel, and the system log to notify the administrator in the event of a system error. *SysMon*, the monitoring thread in the Sun StorageTek 5320 NAS Appliance software, monitors the status of redundant array of independent disks (RAID) devices, Uninterruptible Power Subsystems (UPSs), file systems, head units, enclosure subsystems, and environmental variables. Monitoring and error messages vary depending on model and configuration.

Note: If a table in this appendix has columns with no entries, it means the entries have been deleted.

About SysMon Error Notification

`SysMon`, the monitoring thread in the Sun StorageTek 5320 NAS Appliance, captures events generated as a result of subsystem errors. It then takes the appropriate action of sending an email, notifying the Simple Network Management Protocol (SNMP) server, displaying the error on the liquid crystal display (LCD) panel, writing an error message to the system log, or some combination of these actions. Email notification and the system log include the time of the event.

Reference: UPS Subsystem Errors

Refer to TABLE B-1 for descriptions of uninterruptible power supply (UPS) error conditions.

TABLE B-1 UPS Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Power Failure	**AC Power Failure:** AC power failure. System is running on UPS battery. Action: Restore system power. Severity = Error	EnvUpsOn Battery	U20 on battery	UPS: AC power failure. System is running on UPS battery.
Power Restored	**AC power restored:** AC power restored. System is running on AC power. Severity = Notice	EnvUpsOff Battery	U21 power restored	UPS: AC power restored.
Low Battery	**UPS battery low:** UPS battery is low. The system will shut down if AC power is not restored soon. Action: Restore AC power as soon as possible. Severity = Critical	EnvUpsLow Battery	U22 low battery	UPS: Low battery condition.
Normal Battery	**UPS battery recharged:** The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.

TABLE B-1 UPS Error Messages *(Continued)*

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Replace Battery	**Replace UPS Battery:** The UPS battery is faulty. Action: Replace the battery. Severity = Notice	EnvUps Replace Battery	U23 battery fault	UPS: Battery requires replacement.
UPS Alarms - Ambient temperature or humidity outside acceptable thresholds	**UPS abnormal temperature/humidity:** Abnormal temperature/humidity detected in the system. Action: 1. Check UPS unit installation, OR 2. Contact technical support. Severity = Error	EnvUps Abnormal	U24 abnormal ambient	UPS: Abnormal temperature and/or humidity detected.
Write-back cache is disabled.	**Controller Cache Disabled:** Either AC power or UPS is not charged completely. Action: 1 - If AC power has failed, restore system power. 2 - If after a long time UPS is not charged completely, check UPS. Severity = Warning		Cache Disabled	write-back cache for ctrl *x* disabled
Write-back cache is enabled.	**Controller Cache Enabled:** System AC power and UPS are reliable again. Write-back cache is enabled. Severity = Notice		Cache Enabled	write-back cache for ctrl *n* enabled
UPS is shutting down.	**UPS shutdown:** The system is being shut down because there is no AC power and the UPS battery is depleted. Severity = Critical			!UPS: Shutting down
UPS Failure	**UPS failure:** Communication with the UPS unit has failed. Action: 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR 2. Check the UPS unit and replace if necessary. Severity = Critical	EnvUpsFail	U25 UPS failure	UPS: Communication failure.

Reference: File System Errors

TABLE B-2 describes file system error messages that occur when the file system usage exceeds a defined usage threshold. The default usage threshold is 95 percent.

TABLE B-2 File System Errors

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
File System Full	File system full: File system <name> is *xx*% full. Action: 1. Delete any unused or temporary files, OR 2. Extend the partition by using an unused partition, OR 3. Add additional disk drives and extend the partition after creating a new partition. (Severity=Error)	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is *xx*%.

Reference: RAID Errors

TABLE B-3 displays events and error messages for the RAID subsystem.

TABLE B-3 RAID Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
LUN Failure	RAID LUN failure: RAID LUN *N* failed and was taken offline. Slot *n* is offline. Action: Replace bad drives and restore data from backup. Severity = Error	RaidLunFail	R10 Lun failure	RAID LUN *N* failed and was taken offline. Slot *n* is offline. (Severity=Error)
Disk Failure	Disk drive failure: Disk drive failure. Failed drives are: Slot no., Vendor, Product ID, Size Severity = Error	RaidDiskFail	R11 Drive failure	Disk drive failure. Failed drives are: Slot#, Vendor, Product ID, Size (Severity=Error)
Controller Failure	RAID controller failure: RAID controller *N* has failed. Action: Contact technical support. Severity = Error	RaidController Fail	R12 Ctlr failure	RAID controller *N* failed.

Reference: IPMI Events

Sun StorageTek 5320 NAS Appliance software employs the Intelligent Platform Management Interface (IPMI) board to monitor environmental systems and to send messages regarding power supply and temperature anomalies.

Note: Device locations are shown in Appendix D.

TABLE B-4 describes the IPMI error messages for the Sun StorageTek 5320 NAS Appliance software.

TABLE B-4 IPMI Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Fan Error	Fan Failure: Blower fan *xx* has failed. Fan speed = xx RPM. Action: The fan must be replaced as soon as possible. If the temperature begins to rise, the situation could become critical. Severity = Error	envFanFail trap	P11 Fan *xx* failed	Blower fan *xx* has failed!
Power Supply Module Failure	Power supply failure: The power supply unit xx has failed. Action: The power supply unit must be replaced as soon as possible. Severity = Error	envPowerFail trap	P12 Power *xx* failed	Power supply unit *xx* has failed.
Power Supply Module Temperature	Power supply temperature critical: The power supply unit *xx* is overheating. Action: Replace the power supply to avoid any permanent damage. Severity = Critical	envPowerTemp Critical trap	P22 Power *xx* overheated	Power supply unit *xx* is overheating.

TABLE B-4 IPMI Error Messages *(Continued)*

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Temperature Error	Temperature critical: Temperature in the system is critical. It is xxx Degrees Celsius. Action: 1. Check for any fan failures, OR 2. Check for blockage of the ventilation, OR 3. Move the system to a cooler place. Severity = Error	envTemperatue Error trap	P51 Temp error	The temperature is critical.
Primary Power Cord Failure	Power cord failure: The primary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envPrimary PowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
Secondary Power Cord Failure	Power cord failure: The secondary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envSecondary PowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

APPENDIX **C**

Compliance Archiving Software API

The Sun StorageTek 5320 NAS Appliance product supports compliance data storage as a license key enabled software extension called “Compliance Archiving Software.”

The Compliance Archiving Software is available in a stringent form (referred to as mandatory) and in a less stringent form (referred to as advisory). For overview information about the Compliance Archiving Software, see "About Compliance Archiving Software" on page 136.

This appendix is a technical overview of the features and programming interface for the strict Compliance Archiving Software. It contains the following section:

Note: Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorageTek 5320 NAS Appliance system hardware. In particular, the Sun StorEdge 5300 RAID Expansion Unit arrays should not be connected to any device or network other than a private fibre channel connection to the NAS head and any Sun StorEdge 5300 Expansion Unit expansion enclosures.

Note: To ensure the strongest possible enforcement of your data retention policies, you should also provide for the physical security of your Sun StorageTek 5320 NAS Appliance system. Software-controlled data retention can be no stronger than the physical safeguards used to control access to the system’s hardware.

Compliance Features

The Compliance Archiving Software provides storage-level guarantees regarding the accuracy, integrity, and retention of files. The three major features are described in the following sections:

WORM Files

WORM files enforce stronger access controls than the traditional file access semantics provided by the NFS and CIFS Protocols. When an application designates a file as WORM, the file becomes permanently immutable. WORM files cannot be modified, extended or renamed, regardless of the identity or privileges of the client or user attempting the operation. In addition, WORM files can only be deleted in accordance to the file retention rules described below.

Note: Although these files are called "WORM," in keeping with common parlance for nonrewritable, nonerasable storage, it would be more accurate to call them "permanently read-only." The Sun StorageTek 5320 NAS Appliance does not restrict the way a file is written, or the number of times its contents can be modified before the file is turned into a WORM file.

Per-File Retention Periods

The Compliance Archiving Software associates a retention period for each WORM file. A WORM file cannot be deleted until its retention period has expired. Retention periods may be extended, but never decreased. A new retention period may be assigned to a file whose previous retention period has expired.

Administrative Lock-Down

To ensure the retention and preservation guarantees of WORM files and retention periods, certain system administration features, such as deleting or editing file volumes, are disabled or restricted on compliance-enabled file system volumes. These restrictions affect system administration functions that could be used to circumvent a file's retention (for example, by deleting the file's volume).

Accessing Compliance Functionality

To maintain compatibility with existing client operating systems and applications, the Compliance Archiving Software features are implemented as extensions to the existing file access protocols supported by the Sun StorageTek 5320 NAS Appliance (NFS and CIFS). In particular, the Sun StorageTek 5320 NAS Appliance overloads existing file attributes to indicate the WORM status of a file and the end of its retention period. This simplifies the porting of existing document and record management applications because these metadata fields can be set and viewed using standard client APIs and utilities.

Compliance Volumes

Volumes must be designated as compliance-enabled at the time they are created; existing volumes cannot be converted into compliance volumes. It is possible to have multiple volumes on a single Sun StorageTek 5320 NAS Appliance, only some of which are compliance-enabled.

You should not enable compliance archiving on volumes that will be used by applications (and users) that are not aware of the different data retention semantics enforced by the Compliance Archiving Software.

WORM Files

WORM files cannot be modified or updated. Once a file becomes a WORM file, it is read-only until it is removed.

Creating WORM Files

The Compliance Archiving Software uses a WORM trigger to convert a normal file into a WORM file. When a client application or user executes the trigger action on a file, the Compliance Archiving Software interprets this to mean that the target file should be converted to a WORM file.

The WORM trigger for UNIX clients is setting a file's permission mode to 4000. Client applications or users can invoke this WORM trigger using the chmod command or system call. On receiving this request, the Compliance Archiving Software converts the target file into a WORM file by doing the following:

- Setting the setuid bit
- Clearing any write bits that are set on the file
- Retaining any read access bits on the file

Note: Executable files cannot be made into WORM files. For files created from Windows clients, this means that a file cannot be made into a WORM file if its access control list (ACL) has any access control entries (ACEs) granting execute permission on the file.

In the following example, a file with an access mode of 640 is converted to a WORM file. After the WORM trigger is issued, the file's access mode is 4440.

```
$ ls -l testfile
-rw-r-----   1 smith    staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr-----   1 smith    staff      12139 Dec  2 13:18 testfile
```

The Compliance Archiving Software uses this WORM trigger because it is an operation that is unlikely to be used by existing applications.

The WORM trigger for Windows clients is setting both the read-only and the system bit on a file. Setting these bits will only trigger WORM if neither the archive nor hidden bits are set on the file. The WORM trigger sets the file’s read-only bit, but does not change its system bit.

After a file becomes WORM, it cannot be changed back. From Windows clients, the read-only bit cannot be cleared and the system bit cannot be changed. From UNIX clients, the setuid bit cannot be cleared nor can execute or write permissions be added to the file's access mode.

Compliance-enabled volumes translate these WORM settings between CIFS and NFS. For example, if a UNIX client views a WORM file created by a Windows client, it sees a WORM access mode as described above.

Behavior of WORM Files

WORM files cannot be modified, overwritten, or extended. Any attempt to write to a WORM file will fail and return an error regardless of the client user's identity and access privileges.

Neither the owner of a WORM file nor a user with administrative privileges (even root privileges) can modify a WORM file. WORM files cannot be renamed or changed back to regular (non-WORM) files.

Metadata of WORM Files

The Compliance Archiving Software doesn't allow metadata that contains, protects, describes, or names client data to be modified. Only a restricted subset of metadata fields are allowed to change, depending on operating system, as shown in TABLE C-1.

TABLE C-1 WORM File Metadata That Can and Cannot Be Modified

Operating System	Can	Cannot
UNIX	• Set or clear read permission bits • Change file and group owner	• Enable write and execute bits • Clear setuid bit • Modify size or modification time (mtime)
Windows	• Set or clear read permission bits • Change archive bit • Create and modify access control lists (although a WORM file can never be modified regardless of ACL settings)	• Change the read-only, system, or hidden bits • Modify size or modification time (mtime)

Namespace Restrictions

The Compliance Archiving Software does not allow WORM files to be renamed. Furthermore, non-empty directories cannot be renamed. This rule guarantees that the full pathname of a WORM file cannot change for the lifetime of the file.

Caveats

When a UNIX client sets a file mode to 4000 (invoking the WORM trigger), the resulting access mode on the file will typically not be 4000. This violates the standard semantics of the `chmod` command and system call. As a result, the GNU version of the `chmod(1)` command (used by many Linux distributions) generates a warning message when it is used to issue the WORM trigger. You can ignore this message.

File Retention Periods

Each WORM file has a retention period during which it cannot be deleted. The retention period is specified using a timestamp indicating when the retention period should end. This retention time can be explicitly set by client applications or users. If a retention period is not specified by the client, the Compliance Archiving Software uses the *default retention period* specified for the volume when that volume was created. Any attempt to remove a WORM file prior to the end of its retention period will fail; you can, however, remove a file at any time after the retention period has expired.

Note: Retention periods only govern the ability to remove files. A WORM file can never be modified, regardless of whether its retention period has expired.

Setting Retention Timestamps

The Compliance Archiving System retention timestamps are stored in the access time (atime) attribute of WORM files. Clients typically set the atime attribute prior to changing a file to be read-only. When a file becomes a WORM file, its atime value is rounded down to the nearest number of seconds to determine the retention timestamp.

If the atime attribute represents a time in the past, the file system's default retention period is used to calculate the retention timestamp by adding the default retention period to the current time.

Permanent Retention

Client applications or users can specify that a file should be retained permanently. This permanence is achieved by setting a file's atime to the maximum legal value for a signed 32-bit integer. This value (`0x7fffffff`) is equal to 2,147,483,647. On UNIX systems it is defined as `INT_MAX` in the `limits.h` header file and translates to a timestamp of 03:14:07 GMT, Jan 19, 2038.

Changing Retention Periods

Retention periods can be extended, and new retention periods can be set for files whose retention has expired. This is accomplished by resetting the atime attribute on a WORM file. Such changes are permitted as long as the new value represents a time later than the old retention timestamp.

Access Time Ignored

Because the access time (`atime`) attribute is used by the Compliance Archiving Software to store retention timestamps, that attribute is not updated as a side-effect of standard file system operation, regardless of whether or not a file is a WORM file.

Determining File Status

Client applications and users can determine the retention status of a file by reading the file's metadata using standards tools and APIs. On UNIX clients, for example, a file's attributes can be read via the `stat(2)` system call or viewed using the `ls` command. (`ls -lu` will list files with their access permissions and atime timestamps.)

Behavior of UNIX System Calls

UNIX client applications access the Compliance Archiving Software through their local system call interface. These calls invoke the client NFS implementation, which translates system calls into standard NFS Protocol requests. Because compliance-enabled file systems behave differently than standard NAS file systems, there are corresponding differences in the behavior of the client system calls.

This section describes the standard UNIX system calls that behave differently when a client executes them on a compliance-enabled Sun StorageTek 5320 NAS Appliance share. System calls not listed here behave as normal.

It is important to remember that the interfaces to the Sun StorageTek 5320 NAS Appliance are the NFS and CIFS file access protocols. Thus, this section incorporates both the compliance-related behavior of the Sun StorageTek 5320 NAS Appliance in response to standard protocol requests, and the mapping from system calls to NFS requests. The behavior of these calls has been verified on Solaris operating system clients and should be the same on other UNIX clients.

access(2)

Any check for write permission on a WORM file (that is, a call to `access(2)` where the `amode` argument includes the `W_OK` bit) fails and returns an error (`EPERM`).

chmod(2), fchmod(2)

If the target file is a regular, non-WORM file with none of the execute permission bits set, and the new access permission is 4000 (`S_ISUID`), then the target file becomes a WORM file. When this happens, the file receives a new access mode that is computed by adding the setuid bit to any existing read bits in the file's access mode. More specifically, given an old access mode, oldmode, a file's new access mode after receiving the WORM trigger can be computed as:

```
newmode = S_ISUID | (oldmode & 0444)
```

Executable files cannot be converted to WORM. Applying the WORM trigger (mode 4000) to a file with one or more execute permission bits fails and returns an error (`EACCES`).

Read access bits can be set or cleared on WORM files. Any attempt to enable write or execute permission on a WORM file, to set the setgid bit (`S_ISGID`) or sticky bit (`S_ISVTX`), or to clear the setuid bit on a WORM file fails and returns an error (`EPERM`).

chown(2), fchown(2)

These calls behave the same on WORM files as on non-WORM files.

link(2)

Clients can create new hard links to WORM files. Hard links to a WORM file cannot be removed until the file's retention period ends. (See `unlink(2)`, on page 286).

read(2), readv(2)

Clients can read WORM files. Because retention timestamps are stored in the atime attribute, this value is not updated to reflect read access to WORM files.

rename(2)

Any attempt to rename a WORM file or a non-empty directory on a compliance-enabled file system fails and returns an error (`EPERM`).

stat(2), fstat(2)

When these calls are used to obtain information about regular files, the returned `stat` structure contains compliance-related values. The `st_mode` field contains (as always) the file's mode and permissions. A WORM file has the setuid bit set and no write or execute bits. The `st_atime` field contains a timestamp indicating the end of the file's retention period. If this value is equal to `INT_MAX`, as defined in limits.h, then the file is retained permanently.

unlink(2)

WORM files can only be unlinked if the current time, reflected by the Sun StorageTek 5320 NAS Appliance secure clock, is later than the date stored in the file's atime attribute (that is, the retention timestamp). If this condition does not hold, `unlink(2)` fails and returns an error (`EPERM`).

utime(2), utimes(2)

These calls are used to set a file's access time (atime) and modification time (mtime) attributes. When used on a non-WORM file, they behave normally and provide a mechanism for specifying the retention timestamp before a file is converted to WORM.

When invoked on a WORM file, these calls can be used to extend the file's retention period or to assign a new retention period to a file with expired retention. These calls succeed on a WORM file if the new atime value is greater than (that is, after) the file's existing atime value. If the new atime value is less than or equal to the current atime value, these calls fail and return an error (`EPERM`). When used on a WORM file, the mtime argument is ignored.

write(2), writev(2)

Any attempt to write to a WORM file fails and returns an error (`EPERM`).

Behavior of Windows Clients

The following subsections describe differences in compliance-enabled files for Windows clients.

Creating WORM Files

A regular, non-WORM file can only be converted to a WORM file from Windows if its archive and hidden bits are not set. If these bits are cleared, a Windows client converts the file to a WORM file by setting its read-only and system bits. This WORM trigger will result in setting the file's read-only bit, but will not change the state of the file's system bit.

Metadata Restrictions on WORM Files

Windows clients may change the archive bit on a WORM file. They may not change the read-only, hidden, or system bits. Windows clients can change ACLs on WORM files, but any write permissions in the ACL of a WORM file is ignored. Any attempt to modify the data in a WORM file fails regardless of the permissions in the ACL.

Setting Retention Periods

Like UNIX clients, Windows clients set retention periods by storing retention timestamps in a file's access time (atime) attribute.

Caveats for Windows Clients

The following subsections contain additional information you need to be aware of for Windows clients.

Precautions With Read-Only Bit

It is especially important that compliance-enabled file volumes only be used by Windows applications and users that are aware of the special behavior of WORM files. Many standard Windows utilities for copying files will include the read-only and system bits on a file. If these tools are used to make copies of WORM files on a compliance-enabled volume, the resulting files may become WORM files by virtue of having their read-only and system bits set.

Antivirus Software

Many virus-checking programs attempt to preserve the access time on the files they examine. Typically, those programs read a file's atime before checking it for viruses, and afterwards reset the atime to the value it had before the scan. This can lead to a race condition if the virus-checking program scans a file at the same time that another application is setting a retention time on the file. As a result, the file may wind up with the wrong retention time.

A simple way to avoid this problem is to make sure that virus-checking programs do not run on compliance-enabled file systems or do not run at the same time as applications that create WORM files.

Custom applications can also avoid this issue by using a short default retention period and setting a file's true retention period after applying the WORM trigger.

Other APIs

The Compliance Archiving Software can be accessed through many other client APIs, such as Java, Perl, and C++. All of these languages rely on the same underlying system calls to access shares mounted through NFS or CIFS.

APPENDIX **D**

Sun StorageTek 5320 NAS Appliance Components

This appendix describes components of the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance server (head) hardware. It contains the following sections:

See Chapter 12 for information about components that are identified as customer-replaceable units (CRUs).

Note: The general Sun StorageTek 5320 NAS Appliance features described in this appendix also apply to the Sun StorageTek 5320 NAS Cluster Appliance.

NAS Server

The Sun StorageTek 5320 NAS Appliance server is the basic server unit for all system configurations. FIGURE D-1 shows the front of the server.

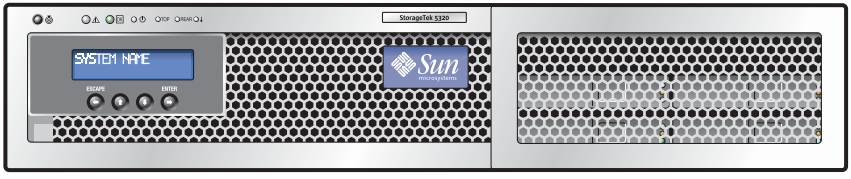


FIGURE D-1 Sun StorageTek 5320 NAS Appliance Front View

Front Panel Buttons and LEDs

The front panel of the server provides a Liquid Crystal Display (LCD) panel, buttons, and LEDs.

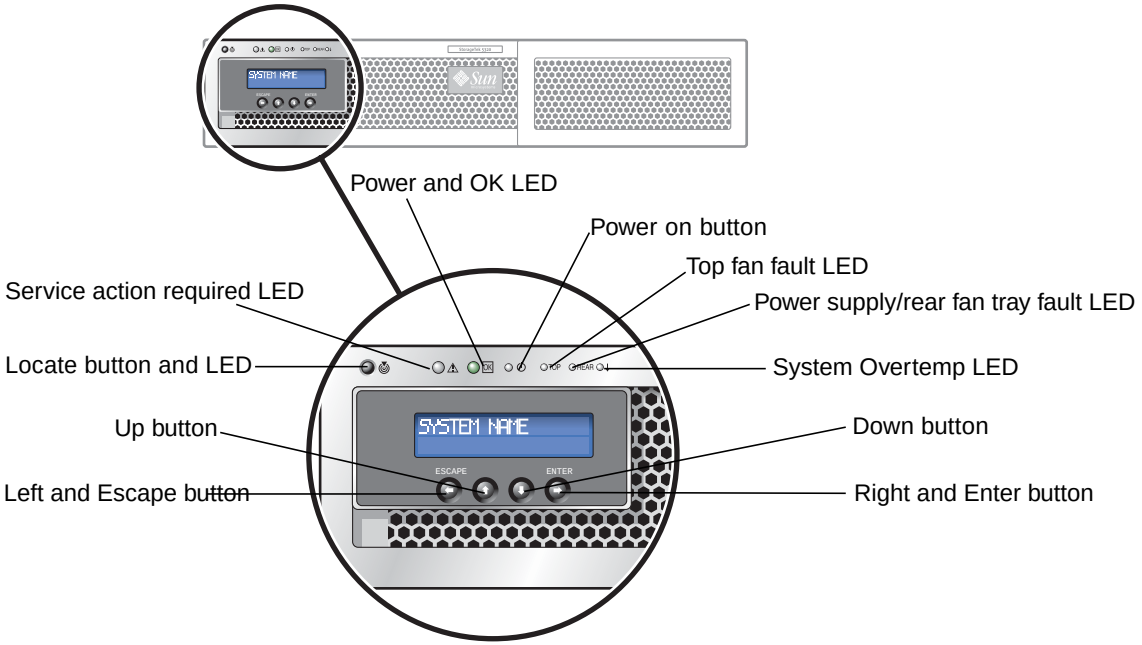


FIGURE 12-22 NAS Server Front Panel Buttons and LEDs

You can use the LCD buttons to navigate through the LCD menu options to perform local basic functions. Basic functions include checking system status, viewing or changing the network configuration settings, and shutting down or rebooting the system.

When you shut down the system using the LCD buttons, you perform a graceful shutdown under operating system control. Remote users can shut down the system through the network using the Web Admin graphical user interface.

Caution: Do not use the power button to shut down the system. Always use the LCD button or remote shutdown procedure described in "Shutting Down the Server" on page 162. Improper shutdown can result in a loss of data.

TABLE D-1 describes the functions of the buttons located on the server front panel.

TABLE D-1 NAS Server Front Panel Buttons

Button	Description
Power on button	Powers on the NAS server. Use a pen tip or similar implement to press and release the recessed button. Always power on the units in the following order: 1. Array expansion units. 2. Array controller units. 3. NAS server.
Left/Escape button	Undo, Backspace, Escape.
Up button	Scrolls up and selects characters, dots, spaces.
Down button	Scrolls down and selects characters, dots, spaces.
Right/Enter button	Accept, Select, Save, Enter.

Status Indicator LEDs

The status LEDs located at the front of the Sun StorageTek 5320 NAS server provide status of server components.

TABLE D-2 describes the LED status indicators that signal current activities taking place in the system.

TABLE D-2 Front LED Status Indicators

LED	Description
Locate button/LED	This LED helps you to identify which system in the rack you are working on in a rack full of servers. • Push and release this button to make the Locate LED blink for 30 minutes. • Hold down the button for 5 seconds to initiate a "push-to-test" mode that illuminates all other LEDs both inside and outside of the chassis for 15 seconds.
Service action required LED	This LED has two states: • Off: Normal operation. • Slow blinking: An event that requires a service action has been detected.
Power/OK LED	This LED has three states: • Off: Server main power and standby power are off. • Blinking: Server is in standby power mode, with AC power applied to only the GRASP board and the power supply fans. • On: Server is in main power mode with AC power supplied to all components.
Top fan fault LED	This LED lights when there is a failed front cooling fan module. LEDs on the individual fan modules indicate which fan module has failed.
Power supply/rear fan tray fault LED	This LED lights when: • Two power supplies are present in the system, but only one has AC power connected. To clear this condition, either plug in the second power supply or remove it from the chassis. • A voltage-related event occurs in the system. For CPU-related voltage errors, the associated CPU Fault LED will also be illuminated. • When the rear fan tray has failed or is removed.
System overtemp LED	• This LED lights when an upper temperature limit is detected.

Back Panel Ports and LEDs

The Sun StorageTek 5320 NAS Appliance server can contain one or two dual port Fibre Channel (FC) host bus adapter (HBA) cards in PCI slot 1 (standard) and PCI slot 0 (optional) for cluster configurations. FIGURE D-2 shows the back of the server.

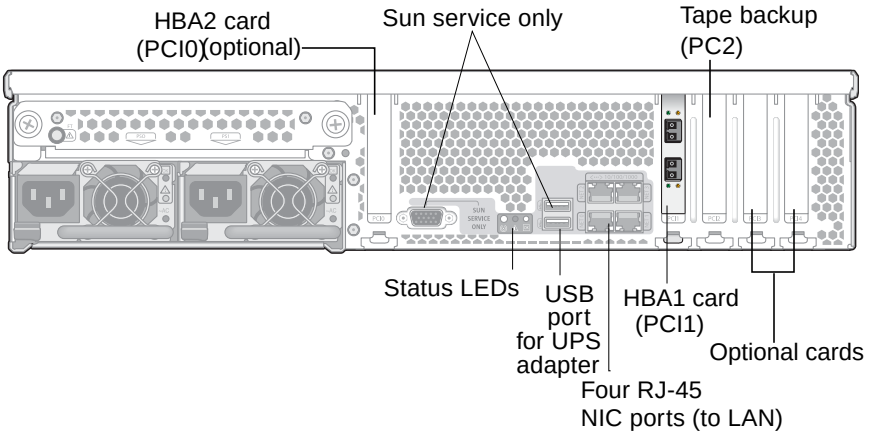


FIGURE D-2 Sun StorageTek 5320 NAS Appliance Back Panel With Single HBA Card

In the Sun StorageTek 5320 NAS Cluster Appliance configuration, two high-availability (HA) servers are sold as a matched pair and are identified in their software serial numbers as server "-H1" and server "-H2." Each server contains two dual port FC HBA cards and can contain other optional cards.

Connecting to an Auxiliary Local UPS

The USB-to-Serial Port Adapter/Convert Cable (included in the ship kit) can be used to connect to a supported local UPS (Uninterruptible Power Supply) device.

Connecting the UPS adapter cable to a supported local UPS device enables the NAS appliance to monitor the state of the UPS. If a power outage occurs, the UPS provides for a graceful shutdown of the system. See "About UPS Monitoring" on page 156 for more information.

You can install the UPS adapter cable without regard to the operating state (ON/OFF) of the NAS server.

To install the UPS adapter cable:

1. Attach the serial port connector side to the supported UPS's serial port interface, following the instructions that came with the UPS device.
2. Attach the USB connector side of the cable to the NAS Appliance's lower USB connector, located on the rear of the unit.

Back Panel LEDs

FIGURE D-3 shows the LEDs located at the back of the server.

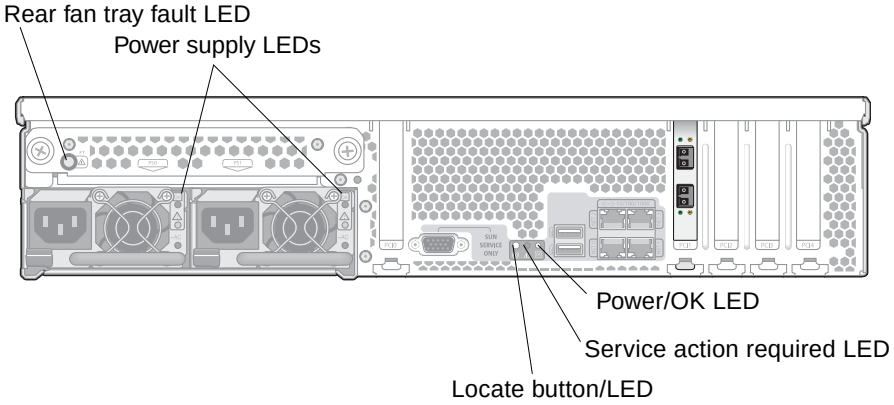


FIGURE D-3 Server Back Panel LEDs

TABLE D-3 describes the functions of the back panel LEDs.

TABLE D-3 Back Panel LED Status Indicators

LED Name	Description
Rear fan tray fault LED	This LED has two states: • Off: Fan module is OK. • Lit (amber): Fan tray has failed.
Power supply LEDs	The power supplies have three LEDs: • Top LED (green): Power supply is OK. • Middle LED (amber): Power supply failed. • Bottom LED (green): AC power to power supply is OK.
Locate button/LED	This LED helps you to identify which system in the rack you are working on in a rack full of servers. • Push and release this button to make the Locate LED blink for 30 minutes. • Hold down the button for 5 seconds to initiate a "push-to-test" mode that illuminates all other LEDs both inside and outside of the chassis for 15 seconds.
Service action required LED	This LED has two states: • Off: Normal operation. • Slow blinking: An event that requires a service action has been detected.
Power/OK LED	This LED has three states: • Off: Server main power and standby power are off. • Blinking: Server is in standby power mode, with AC power applied to only the GRASP board and the power supply fans. • On: Server is in main power mode with AC power supplied to all components.

Server Power Supplies

A system's power supply provides power to all of its components. Power supply systems for all units are autosensing devices with automatic adoption to line voltages from 100 to 240 volts, 50 to 60 Hz.

The power supply system in a server consists of two redundant hot-swappable modules in a 1 + 1 configuration, as shown in FIGURE D-4. Each module is capable of maintaining a load of 500 watts. A minimum of one power supply is required for proper system operation, and two power supplies are required for power redundancy.

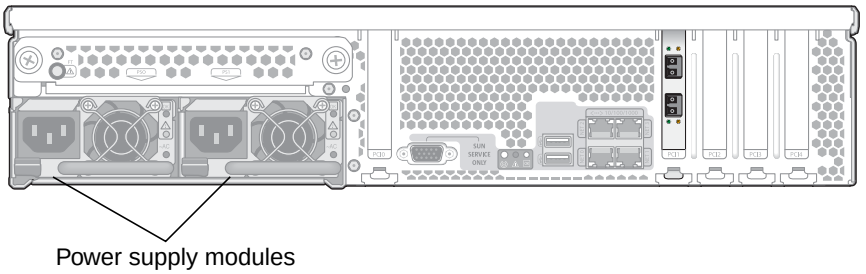


FIGURE D-4 Power Supply Modules

Power supply features include the following:

- 550W output capability
- Internal cooling fans with multi-speed capability
- Built-in load sharing capability
- Built-in overloading protection capability
- Integral handle for insertion/extraction

Direct-Attached Tape Library

A local tape backup drive can be attached to the SCSI port at the lower left of the back of the server.

Note: Make sure that the tape drive is on the list of supported tape units. For the most current information on supported tape devices, contact your Sun sales representative.

The SCSI ID of the tape library must be lower than the tape drive ID. For example, set the library ID to 0 and the drive ID to a nonconflicting value such as 5.

For details about the tape drive system you are using, refer to the documentation that came with the system.

RAID Controller Enclosure and Expansion Enclosure Components

The controller enclosure and expansion enclosures provide storage for the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance.

Controller Enclosures

Sun StorEdge 5300 RAID EU controller enclosures can be used with Fibre Channel expansion enclosures (EU Fs) or with SATA expansion enclosures (EU Ss).

Caution – To add or remove expansion enclosures, you must shut down the system.

The Fibre Channel controller enclosure front panel contains 14 hot-swappable hard drives organized as two 6-drive (5+1) RAID 5 groups, plus two global hot spares. Each 146-gigabyte (raw capacity) drive has an available capacity of 133 gigabytes, for a total available capacity of 1.3 terabytes for the enclosure.

The 300 GB FC drive RAID configuration consists of one 6-drive (5+1) RAID 5 group, one 7-drive (6+1) RAID 5 group, plus one global hot spare.

The controller enclosure used with a SATA system is delivered without hard drives. Instead, all SATA drives are contained in EU S expansion enclosures.

Caution – Do not mix Fibre Channel and SATA disk drives in a controller enclosure or in an array.

Note – In a dual array configuration, one array can contain Fibre Channel disk drives (in the controller enclosure and expansion enclosures) and the other array can contain SATA disk drives (in the expansion enclosures only).

Expansion Enclosures

Expansion enclosures allow you to extend the storage capabilities of the system.

The front panel of each EU F expansion enclosure contains 14 hot-swappable Fibre Channel hard drives organized as two seven-drive (6+1) RAID 5 groups. Each 146-gigabyte (raw capacity) drive has an available capacity of 133 gigabytes, for a total available capacity of 1.6 terabytes per EU F expansion enclosure.

The front panel of the first EU S expansion enclosure contains 14 hot-swappable SATA drives organized as one six-drive (5+1) RAID 5 group, one seven-drive (6+1), plus one global hot spare. Each 400-gigabyte (raw capacity) SATA drive has an available capacity of 360 gigabytes, for a total available capacity of 3.6 terabytes for the first EU S expansion enclosure.

Subsequent EU S expansion enclosures contain 14 hot-swappable SATA hard drives organized as two 7-drive (6+1) RAID 5 groups, providing nearly 4.4 terabytes of additional available capacity.

Caution – Do not mix Fibre Channel and SATA disk drives in an expansion enclosure.

Mixed FC and SATA Expansion Units

Mixed Serial Advanced Technology Attachment (SATA) and Fibre Channel expansion unit (EU) configurations are now supported with the following stipulations.

- Full EUs must consist of all Fibre Channel drives or all SATA drives. Mixing of drive types within an EU is not supported.
- The RAID EU can contain Fibre Channel drives even if the EUs contain SATA drives. The RAID EU cannot contain SATA drives.
- A unique hot-spare must be available for both SATA and Fibre Channel in the same capacity as used in the array.
- LUNs cannot include both SATA and Fibre Channel drives.

Drive Shuttles

Caution – Only Fibre Channel or SATA drives supplied by Sun Microsystems work with the Sun StorageTek 5320 NAS Appliance and Sun StorageTek 5320 NAS Cluster Appliance. For the most current support information, contact your Sun sales representative.

Each drive is encased in its own drive shuttle. These drive shuttles can be individually replaced without shutting down the expansion enclosure, controller enclosure, or Sun StorageTek 5320 NAS Appliance or Cluster.

Caution – Do not mix Fibre Channel and SATA disk drives in an expansion enclosure, a controller enclosure, or an array.

Caution – Hot-swap only one drive shuttle at a time. Confirm that the RAID subsystem has completed any necessary rebuild before removing another drive shuttle.

Caution – Do not update system software or RAID firmware when the RAID subsystem is in critical state or is creating a new RAID set or rebuilding an existing RAID set.

▼ To Locate a Drive or Enclosure

1. **In the Web Administrator navigation panel, select RAID > Manage RAID.**
2. **Click on the Locate Drive or Locate Drive Tray button, which will cause the LCD indicator for the drive or enclosure to flash.**

FIGURE D-5 Fibre Channel Drive Shuttle

▼ To Identify a Drive for Replacement

If you have a disk drive failure, use the log entry to help you identify the specific disk. (You can interpret disk locations in both the system log and diagnostic reports the same way.) The following is a log entry example:

```
Controller 0  enclosure 0  row 0  column 6
```

To interpret such log entries, keep the following points in mind:

- Ignore any channel and target numbers.
- Controller numbering starts at 0. For example, the controllers in the first array (RAID EU) are 0 (slot A) and 1 (slot B), and the controllers in the second array are 2 and 3.
- Enclosure numbering starts at 0 and is relative to the array to which it belongs. For example, if the first array has 2 enclosures they are identified as enclosure 0 and 1.
- Row numbering is always 0 for the Sun StorageTek 5320 NAS Cluster Appliance.
- Column numbering starts at 0 and specifies the slot number in the enclosure.

Thus, you can interpret the example as indicating slot 7 of the first enclosure in the first array.

Note – There is no standard way to identify which array is the first one and which is the second one. Typically, the first HBA port is connected to the first array, the second HBA port is connected to the second array, and so on.

Drive Failure Messages

The following table describes possible drive problems, indications, and corrective actions.

Note – Check the Web Admin GUI and system log to ensure the drive rebuild is completed before performing the following procedures.

TABLE 12-2 Drive Failure Messages

Problem	Meaning	Corrective Action
LED is red	This is an indication of a failed drive.	1. Check to ensure the drive rebuild has completed in the syslog. 2. Verify that an accurate and full system backup is available. If a backup cannot be confirmed, then back up the system immediately. 3. Contact Sun Service to replace the failed drive.
Drive failure message in log or email	This is an indication of has failed or is about to fail	1. Verify that an accurate and full system backup is available. If a backup cannot be confirmed, then back up the system immediately. 2. Contact Sun Service to replace the failed drive.
LCD panel displays `Drive failure` message	This is an indication of a failed drive.	A red light might not exist on this type of error. 1. Verify the drive location through the log or email message. The message indicates the slot of the failing drive. For example, `drive failure slot 9`. 2. Contact Sun Service to replace the failed drive.

Power Supplies

The controller enclosure and expansion enclosures use the same power supply modules.

Power supply module

Controller enclosure

Power supply module Power supply module

Expansion enclosure

Power supply module Power supply module

FIGURE D-6 Power Supply Modules

APPENDIX **E**

Sending a Diagnostic Email Message

The diagnostic email feature enables you to send email messages to the Sun Microsystems Technical Support team or any other desired recipient. Diagnostic email messages include information about the Sun StorageTek 5320 NAS Appliance system configuration, disk subsystem, file system, network configuration, SMB shares, backup and restore processes, `/etc` directory information, system log, environment data, and administrator information.

Every diagnostic email message sent includes all of this information, regardless of the problem.

In a cluster configuration, you must set up diagnostic email for each server in the cluster.

To set up diagnostic email:

1. In the toolbar at the top of the Web Administrator graphical user interface (GUI), click the  button.

   The Diagnostic Email window is displayed.

2. Type a description of the problem in the Problem Description field.

   This is a mandatory entry and is limited to 256 characters.

3. Ensure that the Diagnostics checkbox is selected for at least one email recipient.

   If you need to add or make changes to recipients, see "Setting Up Email Notifications" on page 32.

4. Click Send to send the message.

APPENDIX **F**

Web Administrator Panels

This appendix lists the fields and elements in the panels of the Web Administrator graphical user interface. It includes the following sections:

Anti Virus Configuration Panels

This section describes the fields and elements on the Configure Anti Virus panel.

Configure Anti Virus Panel

This panel enables you to configure antivirus software for the system.

The following table describes the fields and buttons on this panel.

TABLE F-1 Fields and Elements on the Configure Anti Virus Panel

Field	Description
Enable Anti Virus	Select to enable antivirus software on the system.
Scan Mode	Select the mode in which you want antivirus scans to occur: • Scan Suspend (Quarantine Only) - If the Enable Anti Virus checkbox is selected, scans of already quarantined files will not occur and the quarantined files become inaccessible. This option is recommended for temporarily disabling the antivirus software. Otherwise, if you disable the antivirus software by clearing the Enable Anti Virus checkbox, the antivirus software is completely inactive and the quarantined files become accessible. **Note:** Anti-virus protection is not if effect when this option is selected. • Scan after Modify - Scan files only when files are modified. This option offers a compromise between performance and thoroughness of virus protection, enabling fast read access but virus protection only as current as the time of file modification. Later access to the file will not take into account that virus definitions might have changed. • Scan all Access - Scan files when any access to the files is made. This option offers the most thorough virus protection, only allowing access to data that has been scanned by the latest virus definitions.
Scan Engine IP Address	The Internet Protocol (IP) address of the scan engine that you want to set up for virus scanning. There can be up to four scan engines.
Port #	The port number for the scan engine.
Max Conn	The largest number of connections with the scan engine. This number is the number of concurrent threads the scan engine uses to scan the files. The default value is 2.
	Click to remove the selected scan engine from the table or to remove the selected object from the List menu, depending on whether you clicked this button in the Scan Engine IP Address or the List section of the panel.

TABLE F-1 Fields and Elements on the Configure Anti Virus Panel *(Continued)*

Field	Description
Type	The category of objects that you want scanned or that you want ignored by the antivirus software. After clicking one of the following categories, type a value in the List field to specify the object (such as a file extension or client name) to be scanned or ignored: • File Types Included - The types of files to be scanned by the antivirus software. If this field is blank, all file types will be scanned. Entries must be three or fewer characters, and you can use ? for wildcard matching. • File Types Excluded - The types of files to be ignored by the antivirus software. Entries must be three or fewer characters, and you can use ? for wildcard matching. • Exempt Clients - The names or IP addresses of clients to be ignored by the antivirus software. • Exempt Groups - The names of each Windows/NT or Windows Active Directory group (not UNIX group) to be ignored by the antivirus software. Entries can include spaces. • Exempt Shares - The names of each common internet file system (CIFS) share to be ignored by the antivirus software. **Note:** Administrative shares (X$) are always ignored by the antivirus software.
List	The objects that you want scanned or ignored by the antivirus software, depending on the category that is selected in the Type menu. The field at the top of the List section enables you to type a value. The field immediately below lists all previously entered values.
	Click to add the newly typed value from the top field in the List section of the panel to the bottom field in the List section.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configuration Wizard Panels

This section describes the fields and elements on the Configuration Wizard panels of the Web Administrator graphical user interface:

■ "Configuration Wizard Panel" on page 308

- "Confirmation Panel" on page 308
- "Select Environment Panel" on page 309

Configuration Wizard Panel

This is the first screen of the configuration wizard. The configuration wizard is a tool that enables you to configure newly attached systems by entering information in successive windows.

Enter the required information in each window and click Next to continue. At the end of the wizard, you can review the information you have entered and then either edit it before saving it, or discard it by clicking Cancel.

Confirmation Panel

This panel is the last screen of the configuration wizard. It enables you to confirm or discard the information you have entered in the configuration wizard.

Perform one of the following in this window:

- To change the information you have entered before saving it to the system, do the following:

  a. Click the Back button to return to the window in which you want to make changes.

  b. Make your changes and click Next to return to the Confirmation panel.

  c. Click Finish.

     You changes are saved to the system.
- To save the configuration information that you have entered to the system, click Finish.
- To close out of the configuration wizard without saving any information, click Cancel.

Select Environment Panel

This panel enables you to configure the network environment for your newly attached system.

The following table describes the fields and buttons on this panel.

TABLE F-2 Fields and Elements on the Select Environment Panel

Field	Description
Network	
Configure for Windows Only Networks	Select to set a Windows-only network for the system. Select this option if you have no UNIX servers on your network.
Configure for Unix Only Networks	Select to set a UNIX-only network for the system. Select this option if you have no Windows servers on your network.
Configure Both Windows and UNIX Networks	Select to set a mixed Windows and UNIX network for the system. Select this option if you have both Windows and UNIX servers on your network.

File Replicator Panels

This section describes the fields and elements on the File Replicator panels of the Web Administrator graphical user interface:

Add/Edit Mirror Window

This window enables you to add or edit a mirror, depending on whether you accessed the window by clicking Add or Edit.

The following table describes the fields and buttons in this window.

TABLE F-3 Fields and Elements on the Add/Edit Mirror Window

Field	Description
Volume	This field is editable only if the window is in Add mode. Choose the file volume you want to mirror.
Mirror Host	This field is editable only if the window is in Add mode. The name of the server that hosts the mirrored file volume.
IP Address	The Internet Protocol (IP) address to be used for the mirror connection. It is recommended that you use a private network link for mirroring (a link that is not accessible to other devices in the network).
Alternative IP Address	(Optional) The IP address that will be used to maintain the mirror in the event that the first IP address becomes unavailable.
Password	The administrative password that is required to access the mirror host server, if necessary. If there is no administrative password, this field can remain blank.
Mirror Buffer Size (MB)	This field is available only if the window is in Add mode. The size of the mirror buffer. The mirror buffer stores file system write transactions while they are being transferred to the mirror host server. The size of the mirror buffer depends on a variety of factors, but it must be at least 100 MB and must be at least several gigabytes in size. You might want to create a mirror buffer that is approximately 10% of the size of the mirrored file volume. The size you choose is more a function of the write activity to the source file volume than it is of the file volume size. It is important to note that the file volume free space on the active server will be reduced by the allocation size of the mirror buffer.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving your entries.

Manage Mirrors Panel

This panel enables you to add, edit, or break mirrors between the active server and the mirror server. Once a mirror has been broken on the active server, the mirrored file volume can be promoted, or made available for users, on the mirror server.

Note: If a file volume is compliance enabled, you cannot promote the file volume.

The following table describes the fields and buttons on this panel.

TABLE F-4 Fields and Elements on the Manage Mirrors Panel

Field	Description
Volume	The file volume being mirrored.
Active Server	The name or IP address of the server on which the file volume originally exists.
Mirror Server	The name or IP address of the server that is hosting the mirrored file volume.
Sync Status	The status of the mirror: • New – A new mirror is being created. • Creating mirror log – The mirror buffer is being initialized. • Connecting to host – The active server is connecting to the remote mirror server. • Creating extent – Disk partitions are being created on the mirror server. • Ready – The system is ready and waiting for the other system to be ready. • Down – The network link is down. • Cracked – The mirror is cracked. • Syncing Volume – The file volume is being synchronized on the mirror server. • In Sync – The mirror is in sync. • Out of Sync – The mirror is out of sync. • Error – An error has occurred. • Mirror is out of space – The mirror has no more space available for storage use.
Add	(Active server only) Click to mirror a file volume from the active server to the mirror server.
Break	(Active server only) Click to break the selected mirror.
Edit	(Active server only) Click to edit the selected mirror.
Promote	(Mirror server only) Click to launch the Promote Volume window from which you can select the file volume located on the mirror server that you want to promote. **Note:** You can only promote a mirror that has already been broken on the active server.
Change Roles	Click to enable the active volume to function as the mirror volume and vice versa. This does not change the original configuration on each volume. To change the mirror volume role, select the file volume and click Change Roles.

Promote Volume Window

This window enables you to promote a mirrored volume (make it available for users) on the mirror server.

Note: If the volume is compliance enabled, you cannot promote the file volume.

The following table describes the fields and buttons on this panel.

TABLE F-5 Fields and Elements on the Promote Volume Window

Field	Description
Available Volumes	Choose a volume that is available to be promoted (converted from NBD to SFS2 volume).
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Set Threshold Alert Panel

This panel enables you to set the threshold alert for all mirrored file volumes. The threshold alert is the percentage of mirror buffer usage at which a warning is sent to designated recipients.

The mirror buffer stores file system write transactions while they are being transferred to the mirror host server. Increases in write activity to the active server or a damaged network link can cause the transference of write transactions to the mirror server to become backed up in the mirror buffer. If the mirror buffer becomes overrun in this process, the mirror will be cracked and no further transactions will occur between the active server and the mirror server until the mirror is re-established.

To prevent this situation, the software automatically sends warnings when the mirror buffer is filled to certain threshold percentages.

The following table describes the thresholds and buttons on this panel.

TABLE F-6 Fields and Elements on the Set Threshold Alert Panel

Field	Description
	Click and drag this icon to move the threshold value along the scale. As you move the icon, the threshold value that is displayed on the right is updated.
Mirroring Buffer Threshold 1 (%)	The percentage of mirror buffer usage that triggers the first alert. The default value is 70%. This means that when the mirror buffer is 70% full, an alert will be automatically issued.
Mirroring Buffer Threshold 2 (%)	The percentage of mirror buffer usage that triggers the second alert. The default value is 80%.
Mirroring Buffer Threshold 3 (%)	The percentage of mirror buffer usage that triggers the third alert. The default value is 90%.
Alert Reset Interval (Hours)	The amount of time the software will wait before re-issuing an alert that it has already issued. For example, if you set the Mirroring Buffer Threshold 1 to be 10% and the Alert Reset Interval to two hours, the first alert will be issued when the mirror buffer is 10% full. The software will not issue the Threshold 1 alert again for the next two hours. If at that time the mirror buffer usage is still beyond the 10% threshold, the Threshold 1 alert will be issued again. The default value is 24 hours.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

View Mirror Statistics Panel

This panel enables you to view network statistics for mirrored file volumes.

The following table describes the thresholds and buttons on this panel.

TABLE F-7 Fields and Elements on the View Mirror Statistics Panel

Field	Description
Select Volume	
List of Volumes	Select the mirrored file volume for which you would like to see network statistics.
Status	A line of text that describes the status of the mirror.
Transactions (transactions/second)	
Incoming	The incoming transaction statistics for the selected volume, in terms of transactions per second: • Avg - The average number of transactions per second traveling into the active server. • Min - The lowest number of transactions per second that has traveled into the active server. The date and time that this number of transactions occurred is shown on the right, if available. • Max - The largest number of transactions per second that has traveled into the active server. The date and time that this number of transactions occurred is shown on the right, if available.
Outgoing	The outgoing transaction statistics for the selected volume, in terms of transactions per second: • Avg - The average number of transactions per second traveling from the active server to the mirror server. • Min - The lowest number of transactions per second that has traveled from the active server to the mirror server. The date and time that this number of transactions occurred is shown on the right, if available. • Max - The largest number of transactions per second that has traveled from the active server to the mirror server. The date and time that this number of transactions occurred is shown on the right, if available.
Mirror Buffer (transactions)	
Size	The size of the mirror buffer, in terms of transactions (not bytes).
Free	The number of transactions left in the mirror buffer.

TABLE F-7 Fields and Elements on the View Mirror Statistics Panel *(Continued)*

Field	Description
Utilization	The percentage of mirror buffer that is currently being used to hold transactions. If this value approaches 100%,check to make sure that all network links are functioning properly. In the event that a network link goes down, the buffer will be filled up and eventually overrun. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. When the buffer is overrun, the mirror has been cracked. Once the network link has been repaired, the system will automatically begin the mirror update process until the mirrored file volume is back in sync.
Fill Rate	The rate at which the mirror buffer is filling, in terms of transactions per second. If the fill rate is greater than zero, you should check to make sure that all network links are functioning properly. In the event that a network link goes down, the buffer will be filled up and eventually overrun. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. If the buffer is overrun, the mirror has been cracked. Once the network link has been repaired, the system will automatically begin the mirror update process until the mirrored file volume is back in sync.
Network Statistics	
Host	
Hostname	The name of the host, recognized by the network, that will be used for the mirror buffer.
Connected	A line of text that indicates how the host being used by the mirror buffer is connected to the network.
Connected Since	The date on which the host that is being used by the mirror buffer was first connected to the network.
Link	
Status	The link status of the mirror buffer on the network.
Link Quality	The quality of the mirror buffer link on the network.
Errors	Any errors associated with the mirror buffer link on the network.
Timeouts	The number of timeouts for the mirror buffer link on the network.
Drops	The number of drops for the mirror buffer link on the network.
Time of Last Transfer	The time and date at which the last transfer of memory buffer over the network occurred.
Request Control Blocks	
Sent	The number of control blocks sent across the network by the memory buffer.

TABLE F-7 Fields and Elements on the View Mirror Statistics Panel *(Continued)*

Field	Description
Total Bytes	The total bytes of control blocks sent across the network by the memory buffer.
Average Size	The average size of the memory buffer control blocks.
Rate	The rate, per second, of control blocks sent across the network by the memory buffer.
Transfer Rate	
Average (kb/s)	The average rate, in terms of kilobytes per second, at which transfers occur for the memory buffer.
Max (kb/s)	The largest amount of transfers, in terms of kilobytes per second, that occurred for the memory buffer across the network.
When Max Occurred	The date and time when the maximum transfers occurred.
Response Time	
Average (msec)	The average response time of the memory buffer.
Max (msec)	The highest response time of the memory buffer.
When Max Occurred	The date and time at which the highest response time occurred.

File Volume Operations Panels

This section describes the fields and elements on the File Volume Operations panels of the Web Administrator graphical user interface:

- "Schedule Checkpoints Panel" on page 329
- "View Volume Partitions Panel" on page 330

Add/Edit Checkpoint Schedule Window

This window enables you to add or edit a checkpoint schedule, depending on whether you accessed the window by clicking Add or Edit.

Note: A large amount of space and system memory is required for checkpoints. The more checkpoints there are on a system, the greater the effect on system performance.

The following table describes the fields and buttons in this window.

TABLE F-8 Fields and Elements on the Add/Edit Checkpoint Schedule Window

Field	Description
Volume	The volume for which you want to create or edit a checkpoint schedule. If you are editing the checkpoint schedule, you cannot choose a different volume from this menu.
Description	A line of text that describes the checkpoint. This is a mandatory field.
Keep Days + Hours	The period of time (number of days plus number of hours) for which the checkpoint will be retained after being created. In the Days box type an integer value between 0 and 99. From the Hours drop-down menu, choose an integer value between 0 and 23. This is a mandatory field.
Days	The days on which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional days.
AM Hours	The morning hours at which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional items.
PM Hours	The evening hours at which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional items.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit DTQ Setting Window

This window enables you to create or edit a directory in the file system and configure a quota for it.

The following table describes the fields and buttons in this window.

TABLE F-9 Fields and Elements on the Add/Edit DTQ Setting Window

Field	Description
DTQ Name	The name used to identify this directory tree quota.
Dir Name	The name for the new directory. Directory quotas can only be configured for directories created in this field.
Path	The read-only path to the new directory. If you are adding a directory tree quota, you can click the folders in the box underneath this field to populate the Path field. The box shows the directory tree structure for the file volume on which the directory will reside. To view the contents of a folder in this box, click the symbol next to the folder, or double-click the folder itself. Then select the directory that will contain the new directory for which you are setting this quota.
Disk Space Limits	The disk space limit for the directory, between No Limit and Custom: • No Limit - Select to enable unlimited disk space usage for the directory. • Custom - Select to designate a maximum amount of disk space that can be used on the directory. Specify whether the quota is to be determined in megabytes or gigabytes, and type the disk space limit in the Max Value field. Typing a value of 0 (zero) is equivalent to choosing No Limit.
File Limits	The maximum number of files that can be written to this directory, between No Limit and Custom. • No Limit - Select to enable an unlimited number of files to be written to this directory. • Custom - Select to designate a maximum number of files that can be written to this directory. Then type the file limit in the Max Value field.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit Quota Setting Window

This window enables you to add or edit user or group quotas, depending on how you accessed the window (by clicking Add or Edit). Quotas designate disk space and file limits for NT and UNIX users and groups.

The following table describes the fields and buttons in this window.

TABLE F-10 Fields and Elements on the Add/Edit Quota Setting Window

Field	Description
Volume	The volume for which you are adding or editing a user or group quota.
User	The user or group for which you are adding or editing a quota. If you are adding a quota, choose whether the designated user or group belongs to a UNIX or Windows environment by selecting the appropriate Unix or Windows radio button. Then choose the user or group name (and Domain name, for NT users/groups) from the corresponding drop-down menus.
Disk Space Limits	The disk space limits for the selected user or group. Choose one of the following: • Default – Select to set the hard and soft limits to be the same as that of the default user or group, as shown in the "Configure Directory Tree Quotas Panel" on page 321. • No Limit – Select to enable unlimited space usage by the user or group. • Custom – Select to define soft and hard limits for the user or group. Specify whether the quota will be designated in kilobytes, megabytes, or gigabytes. Then type the maximum amount of disk space usage for the user or group in the Max Value field.
File Limits	The maximum number of files a user or group can write to the selected volume. Choose one of the following: • Default – Select to set the hard and soft limits to be the same as that of the default user or group, as shown in the "Configure Directory Tree Quotas Panel" on page 321. • No Limit – Select to enable an unlimited number of files to be written by the user or group. • Custom– Select to define soft and hard limits for the user or group. Specify whether the quota will be designated in kilobytes, megabytes, or gigabytes. Then type the maximum number of files to be written by the user or group in the Max Value field.
Apply	Click to save your changes.

TABLE F-10 Fields and Elements on the Add/Edit Quota Setting Window *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Attach Segments Panel

You can attach segments to the selected primary volume on the Create File Volumes panel or by right-clicking a System Manager object and choosing the appropriate attach segments menu option.

This window or panel enables you to attach segments to an existing primary file volume. Only one segment can be attached at a time.

Note: After a segment is attached, it cannot be detached from a primary file volume. Instead, it becomes a permanent part of that volume.

The following table describes the fields and buttons on this panel.

TABLE F-11 Fields and Elements on the Attach Segments Panel

Field	Description
Existing Volumes	This field is available only from the Create File Volumes panel. Click an existing volume to which you want to attach segments.
Available Segments	A list of the existing file segments (name, LUN, size (MB)) that are available to be attached to primary volumes. If no segments exist, you can create a segment on the "Create File Volumes/Segments Panel" on page 324. For more information, see "Creating a File Volume or Segment Using the Create File Volumes Panel" on page 46.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Directory Tree Quotas Panel

This panel enables you to administer quotas for specific directories in the Sun StorageTek file system. Directory tree quotas determine how much disk space is available for a directory, and how many files can be written to it.

Note: Quotas can only be created and configured for directories that you create from this panel, not for previously existing directories.

The following table describes the fields and buttons on this panel.

TABLE F-12 Fields and Elements on the Configure Directory Tree Quotas Panel

Field	Description
Volume	Choose a primary volume for which you want to configure a directory tree quota.
DTQ Name	The name of the directory tree quota that is applied to a directory on the selected volume.
Max Size (MB)	The largest amount of disk space that can be used in the directory.
Size Used (%)	The percentage of disk space that is currently being used in the directory.
Max File	The largest number of files that can be written to the directory.
File Used	The number of files that are currently written to the directory.
Path	The full path of the directory on the selected volume.
Refresh	Click to update the panel with the latest information about the selected volume.
Add	Click to launch the Add DTQ Setting window. From this window, you can create a new directory on the selected volume and can apply a new directory tree quota to that directory.
Edit	Click to launch the Edit DTQ Setting window. From this window, you can edit the selected directory tree quota.
Delete	Click to delete the selected directory tree quota from the table.

Configure User and Group Quotas Panel

This panel enables you to administer user and group quotas on volumes for NT and UNIX users and groups. User and group quotas determine how much disk space is available to a user or group, and how many files a user or group can write to a volume. Before setting user or group quotas, you must enable quotas for the selected volume on the "Edit Volume Properties Panel" on page 326.

The table displays root, default, and individual quotas for the selected volume. By default, the root user and root group have no hard or soft limits for space or files. The settings for default user and default group are the settings for all users who do not have individual quotas set. For more information about quota limits, see "About Configuring User and Group Quotas" on page 113.

Note: If you want to use user and group quotas, it is recommended that you set up a default disk space or file limit before allowing user or group access. This ensures that users and groups cannot write more data or files than allowed before you configure specific user or group quotas.

The following table describes the fields and buttons on this panel.

TABLE F-13 Configure User and Group Quotas Panel

Field	Description
Volume	Choose an existing volume for which you want to create a user or group quota.
Users	Select to display existing user quotas that are applied to the selected volume.
Groups	Select to display existing group quotas that are applied to the selected volume.
ID	The unique identifier assigned to the user or group quota.
Name	The name of the user or group quota.
Windows Name	The name of the user or group quota as recognized by the Windows environment.
KB Used	The amount of disk space that is currently being used on the volume by the user or group.
Soft KB Limits	A value, equal to or lower than the Hard KB Limits value, that triggers a grace period of seven days. After this grace period is over, the user or group cannot use any more disk space on the volume until the amount of consumed disk space is below the soft limit.

TABLE F-13 Configure User and Group Quotas Panel *(Continued)*

Field	Description
Hard KB Limits	A value, equal to or higher than the Soft KB Limits value, that determines the maximum amount of disk space that can be used on the selected volume by the user or group.
Files Used	The number of files that have been written to the selected volume by the user or group.
Soft File Limits	A value, equal to or lower than the Hard File Limits value, that triggers a grace period of seven days. After this grace period is over, the user or group cannot write any more files to the volume until the number of files already written to the volume is below the soft limit.
Hard File Limits	A value, equal to or higher than the Soft File Limits value, that determines the maximum number of files that can be written to the volume by the user or group.
Refresh	Click to update the panel with the latest information about the user or group quota.
Add	Click to launch the Add Quota Settings window. From this window, you can create a new user or group quota for the selected volume.
Edit	Click to launch the Edit Quota Settings window. From this window, you can edit the selected user or group quota.

Create Checkpoint Window

This window enables you to create a checkpoint.

The following table describes the fields and buttons in this window.

TABLE F-14 Fields and Elements on the Create Checkpoint Window

Field	Description
Volume Name	Choose the volume for which you want to create or edit a checkpoint.
Auto Delete	Select to enable the system to automatically assign a name to the checkpoint, and to remove the checkpoint after the time specified in Keep Days and Hours has elapsed. Specify the following: Keep Days + Hours - The number of days and hours the checkpoint will be retained. In the Days field, type an integer value between 0 and 99. From the Hours drop-down menu, choose an integer value between 0 and 23.

TABLE F-14 Fields and Elements on the Create Checkpoint Window *(Continued)*

Field	Description
Backup	Select to define the default name of the checkpoint as Backup. The checkpoint is used for local backups of the Sun StorageTek 5320 NAS Appliance file system. The checkpoint is not automatically deleted after a specific time period.
Manual	Select to always retain the checkpoint until it is manually deleted. In the Name field, specify the name by which the checkpoint will be saved.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Create File Volumes/Segments Panel

A volume or segment can be created by using the Create File Volumes panel, or by right-clicking System Manager in the navigation pane and selecting the appropriate menu option. You can create a maximun of 31 file volumes per LUN.

Note: A single file volume is limited to 256 gigabytes. However, you can create a larger volume by attaching segments to a primary volume. Up to 63 file segments can be attached.

Before creating a file volume of segments, scan for disks that might have been newly added to the system. To perform this scan, perform one of the following:

- Right-click System Manager in the navigation pane and choose Scan for New Disks.
- Go to File Volume Operations > Create File Volumes in the navigation panel and click Scan for New Disks on the Create File Volumes panel.

The following table describes the fields and buttons on this panel.

TABLE F-15 Fields and Elements on the Create File Volumes/Segments Panel

Field	Description
LUN	Click the logical unit number (LUN) on which you want to create a file volume or segment. A maximun of 31 file volumes can be created per LUN. Clicking a LUN updates the field to the right with a graphical depiction of how the LUN is configured. For more information about the graphical depiction, see the Legend section of the panel.

TABLE F-15 Fields and Elements on the Create File Volumes/Segments Panel *(Continued)*

Field	Description
Name	The name of the file volume or segment. Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).
Partition	If partitions exist, choose the partition on which you want to create a file volume or segment.
Size	The size of the new file volume or segment. From the drop-down menu, choose either MB or GB.
Type	This field is available only on the File Volume Operations > Create File Volumes panel. Choose the type of partition: Primary or Segment.
Compliance Archiving Software	This field is available only if you are creating a file volume on a primary partition and you are on the File Volume Operations > Create File Volumes panel. Click to enable the creation of a mandatory or advisory compliance enforcement volume. Mandatory compliance volumes cannot be deleted.
Legend	Indicators in the graphical depiction of the selected LUN configuration: • Orange - Indicates the primary partition on the LUN. • Light Blue - Indicates the segmented partition on the LUN. • Green - Indicates the mirror on the LUN. • Blue - Indicates that the DOS read-only attribute is applied to the LUN. This DOS read-only attribute is only used on the flash disk for the system volume. • White - Indicates the free space on the LUN.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.
Scan for New Disks	This button is available only if you are on the File Volume Operations > Create File Volumes panel. Click to find disks that have been newly added to the system.

Delete File Volumes Panel

This panel enables you to delete the selected file volume from the configuration.

Note: If the volume is a mandatory compliance volume, it cannot be deleted.

The following table describes the fields and buttons on this panel.

TABLE F-16 Fields and Elements on the Delete File Volumes Panel

Field	Description
Name	The name of the volume that you want to delete.
LUN	The logical unit number (LUN) on which the volume resides. If the volume is made from multiple partitions that reside in multiple LUN. In this situation, the table lists all LUN/partition pairs.
Partition #	The LUN partition on which the volume resides. The volume might reside on multiple partitions that reside in multiple LUNs. In this situation, the table lists all LUN/partition pairs.
Size (MB)	The size of the volume.
Apply	Click to delete the selected volume.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Edit Volume Properties Panel

This panel enables you to edit the properties of a volume, such as its name, checkpoint option, and quota option.

Note: Compliance volumes cannot be renamed or have their compliance feature disabled.

The following table describes the fields and buttons on this panel.

TABLE F-17 Fields and Elements on the Edit Volume Properties Panel

Field	Description
Volumes	Click the existing volume that you want to edit.
Volume Name	The name of the selected volume.
New Name	The new name of the selected volume. Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name can be up to 12 characters in length and must begin with a letter of the alphabet (a–z, A–Z).
Enable Checkpoints	Click to enable checkpoints for the volume. For information about creating checkpoints and about the checkpoint auto delete option, see “Creating File Checkpoints” on page 163.

TABLE F-17 Fields and Elements on the Edit Volume Properties Panel *(Continued)*

Field	Description
Checkpoint Configuration	Options that enable you to configure checkpoints: • Use for Backups - Click to have the backup system create and use a checkpoint named `backup`. • Automatic - Click to have the checkpoint manager create and remove checkpoints automatically based on the configured schedule.
Enable Quotas	Click to enable quotas for the selected volume.
Enable Attic	Click to temporarily save deleted files in the `.attic$` directory located at the root of the volume. By default, this option is enabled. In rare cases on very busy file systems, the `.attic$` directory can be filled faster than it processes deletes, leading to a lack of free space and slow performance. In such a case, you should disable the `.attic$` directory by deselecting this.

Compliance Archiving	These options are available only if you enabled the advisory compliance enforcement version of the compliance archiving software when you created the volume. Options that enable you to configure compliance archiving software:
	• Enabled - An indicator of whether the volume has compliance archiving software enabled.
	  • Mandatory (No Administrator Override) - The volume is mandatory compliant. You cannot configure this volume to be advisory compliant.
	  • Advisory (Allow Administrator Override) - The volume is advisory compliant. If you want to enable mandatory compliance, you must upgrade to the Mandatory Compliant version of the software, and this is a one-time event.
	• Default Retention Period - Click to specify how long write once, read many (WORM) files will be retained on the volume if the client does not provide a retention time. The default retention period for a volume is used if a retention period is not applied to a file before that file is retained. Changing the default retention period for a volume does not affect files that have already been retained.

Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Manage Checkpoints Panel

This panel enables you to view existing checkpoints (one line per checkpoint, per volume), create new checkpoints, and edit and remove existing checkpoints.

The following table describes the fields and buttons on this panel.

TABLE F-18 Fields and Elements on the Manage Checkpoints Panel

Field	Description
Name	The name of the checkpoint.
Volume	The volume for which the checkpoint exists.
Creation Date	The date on which the checkpoint was created.
Expiration Date	The date on which the checkpoint was deleted.
Create	Click to launch the Create Checkpoint window. From this window, you can create a new checkpoint for a volume.
Remove	Click to delete the selected checkpoint from the table.
Rename	Click to launch the Rename Checkpoint window. From this window, you can edit the name of the selected checkpoint.

Rename Checkpoint Window

This window enables you to rename the selected checkpoint.

The following table describes the fields and buttons in this window.

TABLE F-19 Fields and Elements on the Rename Checkpoint Window

Field	Description
Volume Name	The name of the volume for which this checkpoint was created. You cannot edit this field.
Old Name	The name of the checkpoint. You cannot edit this field.
New Name	The new name that you want to assign to the checkpoint.
Apply	Click to save your changes.

TABLE F-19 Fields and Elements on the Rename Checkpoint Window *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Schedule Checkpoints Panel

This panel enables you to schedule the creation of checkpoints for existing file volumes. You can also view, edit, and remove existing checkpoint schedules. For each checkpoint, this panel displays the volume name, a description, the scheduled checkpoint times and days and the amount of time for which the checkpoint will be retained.

The following table describes the fields and buttons on this panel.

TABLE F-20 Fields and Elements on the Schedule Checkpoints Panel

Field	Description
Volume	The volume for which the checkpoint is scheduled.
Description	A line of text that describes the checkpoint.
Days	The days on which the checkpoint is to be created.
AM Hours	The morning hours at which the checkpoint is to be created.
PM Hours	The afternoon and evening hours at which the checkpoint is to be created.
Keep	The period of time (number of days plus number of hours) for which the checkpoint is to be retained after being created.
Add	Click to launch the Add Checkpoint Schedule window. From this window, you can create a new checkpoint schedule for a volume.
Remove	Click to remove the selected checkpoint schedule from the table.
Edit	Click to launch the Edit Checkpoint Schedule window. From this window, you can edit the selected checkpoint schedule.

View Volume Partitions Panel

This panel enables you to view the logical unit numbers (LUNs) available to the system and the volumes that are associated with the LUNs.

The following table describes the fields and buttons on this panel.

TABLE F-21 Fields and Elements on the View Volume Partitions Panel

Field	Description
Volumes	Click the volume to view its location on the existing LUNs.
Legend	Indicators in the graphical depiction of the LUN configuration: • Orange - Indicates the primary partition on the LUN. • Light Blue - Indicates the segmented partition on the LUN. • Green - Indicates mirrored volumes on the LUN. • Blue - Indicates the DOS read-only attribute is applied to the LUN. This DOS read-only attribute is only used on the flash disk for the system volume. • White - Indicates the free space on the LUN. **Note:** The location of the selected volume on a LUN is indicated by diagonal lines (///).
Lun	The name of the LUN on which the selected volume resides.
Partition	The LUN partition on which the volume resides.
Use (%)	The percentage of space used on the volume.
Type	The type of volume, such as primary or segmented.
Free (MB)	The amount of space available on the volume for storage use.
Capacity (MB)	The total amount of space on the volume for storage use.

High Availability Panels

This section describes the fields and elements on the High Availability panels of the Web Administrator graphical user interface:

- "Enable Failover Panel" on page 331
- "Recover Panel" on page 332
- "Set LUN Path Panel" on page 333
- "Set Primary Path Window" on page 334

Enable Failover Panel

Note: This panel is available only to Sun StorageTek 5320 NAS Cluster Appliances.

This panel enables you to enable head failover for your Sun StorageTek 5320 NAS Cluster Appliance. A failover occurs when one of the heads in a dual server system fails. The functioning head automatically takes over or manages the Internet Protocol (IP) addresses and logical unit numbers (LUNs) formerly managed by the failed head. When the failed head is manually brought back online, original ownership or control of the said LUNs and IP address is restored in a process called failback or recovery. For more information about failover, see "About Enabling Failover" on page 19.

Note: When a failed server (head) is brought back online, you must initiate the recovery process from the Recover panel. For more information, see "Initiating Recovery" on page 22.

The following table describes the fields and buttons on this panel.

TABLE F-22 Fields and Elements on the Enable Failover Panel

Field	Description
Automatic Failover	Click to have the system automatically initiate failover in the event of a head failure.
Head Status	An indicator of the health of the head.
Link Failover	
Enable Link Failover	Click to enable link failover, which ensures that head failover occurs when any network interface that is assigned a "primary" role fails. This type of failure is referred to as a "link down" condition. If the partner's network link is down, the head that wants to induce the failover must wait the specified amount of time after the partner head re-establishes its network link. **Note:** The system must be rebooted after enabling or disabling link failover for the change to take effect.
Down Timeout	The number of seconds a head waits, in the event that the network link on one head becomes unreliable and the network link on its partner head is healthy, before inducing head failover.
Restore Timeout	The number of seconds the partner head's primary link must be up in order for the failover to take place. The Restore Timeout is used only when a link down induced failover is initiated but aborted due to the partner head's primary link being down.

TABLE F-22 Fields and Elements on the Enable Failover Panel *(Continued)*

Field	Description
Partner Configuration	
Name	The name of the partner server.
Gateway	The gateway IP address of the partner server.
Private IP	The IP address reserved for the heartbeat connection between the two servers (heads). The IP address cannot be changed.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Recover Panel

Note: This panel is available only to Sun StorageTek 5320 NAS Cluster Appliances.

This panel enables you to initiate recovery after a failed server (head) is brought back online. You must verify that the failed head or controller is operable and online before proceeding to the recovery process.

The following table describes the fields and buttons on this panel.

TABLE F-23 Fields and Elements on the Recover Panel

Field	Description
Current RAID Configuration	
Head 1	The name of the server, designated as Head 1, that you want to recover.
Head 2	The name of the server, designated as Head 2, that you want to recover.
(NEW) Restore RAID Configuration	
Controller 0/Head 1	Depending on your configuration, this is either the LUN mapping for controller 0 or the LUN mapping for Head 1.
Controller 1/Head 2	Depending on your configuration, this is either the LUN mapping for controller 1 or the LUN mapping for Head 2.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.
Apply	Click to save your changes.

TABLE F-23 Fields and Elements on the Recover Panel *(Continued)*

Field	Description
Recover	Click to Recover the selected

Set LUN Path Panel

This panel enables you to define, edit, and restore, the logical unit number (LUN) paths for a file volume.

A LUN path is a designation of the hardware route (from head to RAID controller) used to access a file volume in a LUN. Every file volume has two LUN paths. The alternate path is used when the primary path fails.

The following table describes the fields and buttons on this panel.

TABLE F-24 Fields and Elements on the Set LUN Path Panel

Field	Description
LUN	The LUN on which file volumes are located.
Volumes	The specific file volumes on the LUN.
Active Path (HBA/SID)	The currently active hardware path over which the LUN communicates with the system. Hardware paths are identified by the host bus adapter (HBA) number, starting with 1, and the Small Computer Systems Interface (SCSI) identifier (ID) number of the first drive in the LUN, which is the controller. For example, `1/1` designates HBA 1 and SCSI controller target 1.
Primary Path (HBA/SID)	The preferred hardware path over which the LUN communicates with the system. The primary path is also the path to which a LUN path can be "restored." If a primary path is not specified, the system uses the first available path.
Alternate Path (HBA/SID)	The alternate hardware path over which the LUN can communicate with the system if the primary path fails.
Edit	Click to launch the Primary Path window. From this window, you can edit the primary path for the selected volumes.
Restore	Click to restore the active path to the primary path for the selected volumes.
Auto-assign LUN Paths	Click to have the software automatically assign LUN paths to the selected volumes.

Set Primary Path Window

This window enables you to define the primary path, which is the hardware route that the software uses to send information to the shared LUN. The secondary path is used when the primary path fails.

The following table describes the fields and buttons on this panel.

TABLE F-25 Fields and Elements on the Set Primary Path Window

Field	Description
LUN Name	The read-only name of the LUN for which you are setting the primary path.
Primary Path	The host bus adapter (HBA) and Small Computer Systems Interface (SCSI) identifier (ID) that define the path. Choose the path you want from the drop-down menu.
Volumes	The read-only name of the volume on the selected LUN.
Text box	A line of text that indicates the HBAs, SIDs, and the status of the available paths.
Apply	Click to save your changes.
Cancel	Click to clear the fields of any entries and close out of the window without saving the changes.

iSCSI Configuration Panels

This section describes the fields and elements on the iSCSI Configuration panels of the Web Administrator graphical user interface:

- "Add/Edit iSCSI Access Window" on page 335
- "Add/Edit iSCSI LUN Window" on page 336
- "Configure Access List Panel" on page 337
- "Configure iSCSI LUN for MS-Exchange Panel" on page 338
- "Configure iSNS Server Panel" on page 338

Add/Edit iSCSI Access Window

This window enables you to create or edit an Internet Small Computer Systems Interface (iSCSI) access list, depending on whether you accessed the window by clicking Add or Edit. An iSCSI access list defines which iSCSI initiators have access to a logical unit number (LUN).

The following table describes the fields and buttons in this window.

TABLE F-26 Fields and Elements on the Add/Edit iSCSI Access Window

Field	Description
Name	The name of the access list. The name can consist of one or more characters and can contain alphanumeric (a–z, A–Z, 0–9) characters, periods (.), hyphens (-), or colons (:).
CHAP Initiator Name	The full name of the Challenge Handshake Authentication Protocol (CHAP) initiator that is configured by the iSCSI initiator software. The default CHAP initiator name for a Windows iSCSI client is: `iqn.1991-05.com.microsoft:iscsi-winxp` If you leave this field blank, CHAP authorization will not be required. Refer to the iSCSI initiator documentation for more information.
CHAP Initiator Password	The CHAP initiator password.
Initiator IQN Name	The initiator iSCSI Qualified Name (IQN) name. If you leave this field blank, any initiator can access the target. The name can consist of one or more characters and can contain alphanumeric (a–z, A–Z, 0–9) characters, periods (.), hyphens (-), or colons (:).
	Click to add the Initiator IQN name to the list of initiators that can access the target LUN.
Initiator IQN List	The list of initiators that can access the target LUN.
	This button is available only if the target LUN that is associated with the selected initiator is inactive. Click to remove the selected initiator from the list. The initiator then no longer has access to the LUN.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit iSCSI LUN Window

This window enables you to add or edit an Internet Small Computer Systems Interface (iSCSI) logical unit number (LUN), depending on whether you accessed the window by clicking Add or Edit. An iSCSI LUN can be accessed by iSCSI initiators.

Before adding or editing an iSCSI LUN, ensure that you have created an access list for the LUN. For more information, see "Creating an iSCSI Access List" on page 55.

The following table describes the fields and buttons in this window.

TABLE F-27 Fields and Elements on the Add/Edit iSCSI LUN Window

Field	Description
Name	The name of the iSCSI LUN. The name can consist of one or more characters and can contain alphanumeric (a–z, A–Z, 0–9) characters, periods (.), hyphens (-), or colons (:). The target name you specify will be prefixed with the full iSCSI Qualified Name (IQN) name according to the following naming convention: `iqn.1986-03.com.sun:01:`*mac-address*`.`*timestamp*`.`*user-specified-name* For example, if you type the name `lun1`, the full name of the iSCSI target LUN is: `iqn.1986-03.com.sun:01:`*mac-address*`.`*timestamp*`.`**`lun1`** Note: The timestamp is a hexadecimal number representing the number of seconds after 1/1/1970.
Alias	(Optional) A brief description about the target LUN.
Volume	The name of the volume on which the iSCSI LUN is to be created.
Capacity	The maximum size for the LUN, in bytes, kilobytes, megabytes, or gigabytes.
Sparse	Select the Yes checkbox to create a sparse LUN. A sparse LUN sets the file size attribute to the specified capacity, but the disk blocks are not allocated until data is written to the disk. For more information, see "About iSCSI Sparse LUNs" on page 56. If you create a non-sparse LUN, disk blocks will be allocated based on the capacity of the LUN you are creating. When creating non-sparse iSCSI LUNs, allow approximately 10% extra space on the volume for file system metadata. For example, a 100-GB iSCSI LUN should reside on a 110-GB volume to allow non-sparse LUN creation. For more information about deciding to use sparse or non-sparse LUNs, see "About iSCSI Sparse LUNs" on page 56.

TABLE F-27 Fields and Elements on the Add/Edit iSCSI LUN Window *(Continued)*

Field	Description
Access	Choose the existing access list for this LUN from the drop-down list.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Configure Access List Panel

This panel enables you to create access lists, which define the Internet Small Computer Systems Interface (iSCSI) initiators that can access a logical unit number (LUN). This panel also enables you to view, edit, and remove existing access lists.

The following table describes the fields and buttons on this panel.

TABLE F-28 Fields and Elements on the Configure Access List Panel

Field	Description
Name	The name of the access list.
CHAP Initiator Name	Enter the full name of the Challenge Handshake Authentication Protocol (CHAP) initiator that is configured by the iSCSI initiator software. The default CHAP initiator name for a Windows iSCSI client is: `iqn.1991-05.com.microsoft:iscsi-winxp` If you leave this field blank, CHAP authorization will not be required. Refer to the iSCSI initiator documentation for more information.
Add	Click to launch the Add iSCSI Access window. From this window, you can add a new access list.
Remove	Click to remove the selected access list from the Configure Access List table.
Edit	Click to launch the Edit iSCSI Access window. From this window, you can edit the selected access list.

Configure iSCSI LUN for MS-Exchange Panel

This panel enables you to add Internet Small Computer Systems Interface (iSCSI) logical unit numbers (LUNs) that iSCSI initiators can access. You can also view, edit, and remove existing iSCSI LUNs on this panel.

The following table describes the fields and buttons on this panel.

TABLE F-29 Fields and Elements on the Configure iSCSI LUN for MS-Exchange Panel

Field	Description
Name	The name of the iSCSI LUN.
Alias	A brief description about the target LUN.
Volume	The name of the volume on which the iSCSI LUN is to be created.
Add	Click to launch the Add iSCSI LUN window. From this window, you can add a new iSCSI LUN.
Remove	Click to remove the selected iSCSI LUN from the Configure Access List table.
Edit	Click to launch the Edit iSCSI LUN window. From this window, you can edit the selected iSCSI LUN.

Configure iSNS Server Panel

This panel enables you to specify the Internet Storage Name Service (iSNS) server to be used by the software.

The following table describes the fields and buttons on this panel.

TABLE F-30 Fields and Elements on the Configure iSNS Server Panel

Field	Description
iSNS Server	The Internet Protocol (IP) address or Domain Name Service (DNS) name of the iSNS server.
Apply	Click to save your changes.

TABLE F-30 Fields and Elements on the Configure iSNS Server Panel *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Monitoring and Notification Panels

This section describes the fields and elements on the Monitoring and Notification panels of the Web Administrator graphical user interface:

Configure SNMP Panel

This panel enables you to configure Simple Network Management Protocol (SNMP) monitoring. SNMP is an industry standard for coordinating the operation of diverse network devices.

The following table describes the fields and buttons on this panel.

TABLE F-31 Fields and Elements on the Configure SNMP Panel

Field	Description
Enable SNMP	Click to enable SNMP monitoring for the system.

TABLE F-31 Fields and Elements on the Configure SNMP Panel *(Continued)*

Field	Description
Server SNMP Community Name	The name of the SNMP community to which the system belongs.
Contact Info	The name of the person who is responsible for this system.
System Location	The network location of the system. This location can be physical or logical.
Destination IP Address	The transmission control protocol/Internet Protocol (TCP/IP) address for the server that is designated as an SNMP trap destination, in the event of system errors.
Port #	The port to which the system will send traps. The default value is port 162.
Version	The SNMP protocol version (either 1 or 2).
Community	The community string for the trap destination.
Enable	Click to enable this target address to become a trap destination.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure System Auditing Panel

This panel enables you to configure system auditing. You can set up system auditing so that records of particular system events are stored in separate audit log files.

Note: There is no Web Administrator graphical user interface support for reading or removal of audit logs. To read audit log files, you must use the `praudit` command, which converts the binary information in the audit logs into readable text.

The following table describes the fields and buttons on this panel.

TABLE F-32 Fields and Elements on the Configure System Auditing Panel

Field	Description
Enable System Auditing	Select to enable system auditing.
Log File Configuration	

TABLE F-32 Fields and Elements on the Configure System Auditing Panel *(Continued)*

Field	Description
Store Log Files to Volume	The volume on which system audit log files are stored. **Note:** Selectable volumes are non-system volumes. You must create special purpose audit volumes. (For instructions, see "Creating a File Volume or Segment Using the Create File Volumes Panel" on page 46.)
Max Log File Size (1 to 1024)	The largest size to which a system audit log file can grow, from 1 to 1024 megabytes.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Display System Log Panel

This panel enables you to selectively view, print, and save system log messages. The system software logs and displays the following types of events:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug

The following table describes the fields and buttons on this panel.

TABLE F-33 Fields and Elements on the Display System Log Panel

Field	Description
File	The name of the log file that you are viewing. This field is blank when you are viewing the system log file.
Date	The date upon which the event occurred.
Time	The time, in military format, at which the event occurred.
Description	A line of text that describes the event.

TABLE F-33 Fields and Elements on the Display System Log Panel *(Continued)*

Field	Description
Event Types	Click the types of events that you want displayed on this panel. To update the log file so that it displays only the selected event types, click Refresh.
Refresh	Click to update the log with the latest information.
Print	Click to print the log.
Save As	Click to save the log as an HTML file on your local system.
Open	Click to open a different log file for display on this panel.
Silence Alarm	This button is available only for Sun StorageTek 5210 systems. Click to silence the redundant array of independent disks (RAID) alarm.

Set Up Email Notification Panel

This panel enables you to set the name of the Simple Mail Transport Protocol (SMTP) server and designate email notification recipients. In the event of a system error, the system will send a detailed email message to the designated recipients through the SMTP server.

Recipient email addresses are displayed in the List box. When an error is detected, the system logs the error in the system log file and sends email notifications and warnings to the listed recipients.

Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-34 Fields and Elements on the Set Up Email Notification Panel

Field	Description
SMTP Server Name	The name of the SMTP server.
Mail From	The email address of the sender.
Email Address	The email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.

TABLE F-34 Fields and Elements on the Set Up Email Notification Panel *(Continued)*

Field	Description
List	
	Click to add the new recipient to the list of recipients.
	Click to remove the selected recipient from the list of recipients.
Recipient	The email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.
Notification Level	
Errors	Select to notify recipients of system errors but not system warnings.
Errors and Warnings	Select to notify recipients of all system warnings and errors.
None	Select to disable email notifications. The Sun StorageTek server will not send any notifications.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Logging Panel

This panel enables you to set up logging for the system. You can enable remote logging if your system includes a `syslogd` UNIX server.

Before you can enable remote logging, the following conditions must be met:

- The system must be able to send the system log to this remote `syslogd` server. (See "Setting Up Logging" on page 33.)
- DNS settings must be configured.

The following table describes the fields and buttons on this panel.

TABLE F-35 Fields and Elements on the Set Up Logging Panel

Field	Description
Enable Remote Syslogd	Click to enable the system message logger and its designated server.
Server	The name of the server to which the system log will be sent.
Facility	The application or system component that generates log messages. All messages that are sent to the `syslogd` server will have this facility value. Select the types of events for which you want to generate log messages: • Emergency • Warning • Alert • Notice • Critical • Info • Error • Debug
Enable Local Log	Click to enable local system logging, which enables the system to save log messages locally.
Local File	The path and file name of the system log. The log cannot be written to the `/cvol` directory.
Archives	The maximum number of archive files, from 1 to 9.
Size	The maximum allowable size, in kilobytes, for each archive file. The allowable range is from 100 through 999,999 kilobytes.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up UPS Monitoring Panel

This panel enables you to set up uninterruptible power supply (UPS) monitoring (not UPS management). For more information about the UPS events that can be monitored, see "About UPS Monitoring" on page 156.

Note: Before you can enable UPS monitoring on this panel, the UPS monitoring service must be connected to the system. Otherwise, the UPS monitoring system will notify you that there is a UPS failure.

The following table describes the fields and buttons on this panel.

TABLE F-36 Fields and Elements on the Set Up UPS Monitoring Panel

Field	Description
Enable UPS Monitoring	Click to enable UPS monitoring for the system. In order to work properly, the UPS monitoring service must be connected to the system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

View Fan Status Panel

This panel enables you to view the status and revolutions per minute (RPMs) of each fan assembly in the head unit of the system.

The following table describes the fields and buttons on this panel.

TABLE F-37 Fields and Elements on the View Fan Status Panel

Field	Description
Fan	The fan for which you are viewing a status condition.
Status	A visual indicator of the status of the fan: • Green diamond - The RPMs are normal for this fan. • Red diamond - The RPMs have exceeded an acceptable range for this fan. If the revolutions per minute fall below 1800 for a fan, an email notification will be sent to the designated email recipients. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 32.
RPM	The number of RPMs for the fan.

View File Volume Usage Panel

This panel enables you to view how each Sun StorageTek file volume is being used.

The following table describes the fields and buttons on this panel.

TABLE F-38 Fields and Elements on the View File Volume Usage Panel

Field	Description
Name	The name of the file volume.
Capacity	A graphical representation of the amount of space used on the file volume and the amount of space available to be used.
Volume Status	The status of the volume: read/write (r/w) or read only (r/o).
Requests	The number of requests processed for the volume since the volume was mounted.
Active	The number of requests processed for the volume in the last ten minutes.

View Power Supply Status Panel

This panel enables you to view the current status of all power supplies for the system.

The following table describes the fields and buttons on this panel.

TABLE F-39 Fields and Elements on the View Power Supply Status Panel

Field	Description
Power Supply	The power supply for which you are viewing a status condition.
Status	A visual indicator of the status of the power supply: • Green diamond - The voltage and temperature levels are normal for this power supply. • Red diamond - The voltage and temperature levels have exceeded the acceptable range. An email will be sent to the designated email recipients to notify them of this condition. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 32.

TABLE F-39 Fields and Elements on the View Power Supply Status Panel *(Continued)*

Field	Description
Description	A line of text that describes the status condition of the power supply.

View Temperature Status Panel

This panel enables you to view the temperature of the sensors in the head unit of the system.

The following table describes the fields and buttons on this panel.

TABLE F-40 Fields and Elements on the View Temperature Status Panel

Field	Description
Sensor	The sensor for which you are viewing a status condition.
Status	A visual indicator of the status of the sensor: • Green diamond - The sensor is operating within the normal temperature range. • Red diamond - The temperature has exceeded the acceptable range. If the temperature rises above 55 degrees Celsius (131 degrees Fahrenheit), an email will be sent to the designated email recipients. For more information about setting up email notifications, see "Setting Up Email Notifications" on page 32.
Value	The temperature of the sensor.

View Voltage Regulator Status Panel

This panel enables you to view the current readings for voltage regulators on the system. Voltage regulators are devices or circuits that regulate the voltage fed to a microprocessor.

The following table describes the fields and buttons on this panel.

TABLE F-41 Fields and Elements on the View Voltage Regulator Status Panel

Field	Description
Voltage Regulator	The voltage regulator for which you are viewing a status condition.
Status	A visual indicator of the status of the power supply: • Green diamond - The voltage level is normal for this voltage regulator. • Red diamond - The voltage level has exceeded the acceptable range for this voltage regulator. An email will be sent to the designated email recipients to notify them of this condition. For more information about setting up email notifications, see "Setting Up Email Notifications" on page 32.
Current Value	The number of volts currently being fed to the microprocessor.

Network Configuration Panels

This section describes the fields and elements on the Network Configuration panels of the Web Administrator graphical user interface:

Bond NIC Ports Panel

This panel enables you to add, edit, remove, and recover network interface card (NIC) port bonds.

The following table describes the fields and buttons on this panel.

TABLE F-42 Fields and Elements on the Bond NIC Ports Panel

Field	Description
Bond ID	The unique NIC port bond designation for this bond.
Type	The type of bond, which can be either of the following: • Port aggregation – Also known as “channel bonding” or "trunking." Lets you scale network I/O by joining NIC ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth. You must have a minimum of two available NIC ports for port bonding. **Note:** All NIC ports in an aggregation bond must be of the same type of interface card (such as, Fast Ethernet with Fast Ethernet), be connected to the same subnet, and be connected to adjacent ports. For systems that use switches, the switches must support port (or channel) bonding. • High availability – Provides NIC port failover. Multiple NIC ports can be bonded to a primary port as backup ports. When the primary port fails, the software automatically switches to the backup port at the top of the list of high-availability bonded ports. If that port also fails, the port next on the list is used, and so on. **Note:** NICs in a high availability bond do not have to be the same type of interface card or be connected to the same subnet.
Status	Color coded statuses: • Normal (green) • Failover (yellow) • Down (red) – This occurs if the ports fail, if the primary port and slave ports in a high-availability bond failure, or if failover is unsuccessful.
IP Address	The Internet Protocol (IP) address designated for the port bond.
Subnet Mask	The subnet mask associated with the bond.
Broadcast Address	The broadcast address associated with the bond.
Slaves	Any slave ports in the bond.
Create	Click to launch the Create Port Bond window. From this window, you can create a new port bond.
Edit	Click to launch the Edit Port Pond window. From this window, you can edit the selected port bond.
Remove	Click to remove the port bond from the table.
Recover	Click to recover from a NIC port failover. Clicking Recover starts the recovery process. The failed NIC port must be online before you attempt to recover.

Configure Network Adapters Panel

This panel enables you to configure Dynamic Host Configuration Protocol (DHCP) for the system or specify the Internet Protocol (IP) address, netmask, and broadcast for each network controller. In addition, this panel enables you to add IP aliases for each network interface card (NIC).

The following table describes the fields and buttons on this panel.

TABLE F-43 Fields and Elements on the Configure Network Adapters Panel

Field	Description
Enable DHCP	Click to enable DHCP. DHCP enables the system to dynamically acquire an IP address from the DHCP server. If you want to manually configure the static IP address, subnet mask, and/or gateway IP, do not select this checkbox.
Adapter	A list of the existing NIC ports. If you have already created a port bond, that port bond is displayed in this menu. Ports that are not bonded are labeled Port *x*, whereas ports that are bonded are labeled Bond x. **Note:** If ports are bonded, you cannot create alias IP addresses for each port, but instead you create the alias for the bond. For example, if you have bonded Port 2 and Port 3 to form Bond 1, you cannot add alias IP addresses to Port 2 or Port 3. You can only add aliases to Bond 1.
IP Address	The primary IP address for the NIC port that is selected in the Adapters menu.
Netmask	An indicator that shows which portion of an IP address identifies the network address and which portion identifies the host address.
Broadcast	The read-only broadcast address for the NIC port that is selected in the Adapters menu. The broadcast address is the IP address used to send broadcast messages to the subnet.

TABLE F-43 Fields and Elements on the Configure Network Adapters Panel *(Continued)*

Field	Description
Role	The NIC role for the NIC port that is selected in the Adapters menu. Valid roles are the following: • Primary – The NIC port role that designates an active network port and is an integrated piece of the failover process. When you assign this role to a network adapter, the partner head (head 2) holds the IP address that is assigned to this adapter as a backup alias IP address. The reverse occurs when you supply an alias IP address on the partner head. The partner IP address is held as a backup alias IP address by this head (head 1). Should failover occur, the healthy head activates the partner head alias IP addresses, allowing network access to continue as if the failed head were still active. **Note:** In dual server (2 head) systems, the heartbeat NIC's role is `private`. For dual server systems that have the File Replicator option enabled, the designated NIC port has the role of Mirror. A NIC port that is part of a bond (high availability) can have a Main or Bkup1 to Bkup7 role. • Independent – The NIC port role that designates an active network port, but does not participate in the failover process. Independent NIC ports are typically used for remote backup. You cannot aggregate independent NIC ports or add alias IP addresses to them. There can be any number of independent NIC port roles assigned, but it is recommended that you assign only one per head. • Mirror – This option is available only for dual server systems. The NIC port role that shows that the port connects this server to another server in order to mirror file volumes. • Private – This option is available only for Sun StorageTek 5320 NAS Cluster Appliance configurations. The NIC port role that is reserved for the heartbeat, which is a dedicated network link that constantly monitors the status of the other server (head). Each server (head) has only one private port.

TABLE F-43 Fields and Elements on the Configure Network Adapters Panel *(Continued)*

Field	Description
Interface	Interface-specific information that applies to the selected NIC port: • Description – A line of text that describes the selected adapter. • H/W Address – The Hardware (H/W) or Media Access Control (MAC) address, which is a unique address in hexadecimal format, that is used by network software to distinguish this network card from others on the network. This address is encoded on the network card at the factory. • Speed – The speed (Mb data/sec) at which data is transmitted over the network. • MTU/Max MTU – The current Maximum Transmission Unit (MTU) of the selected adapter. MTU is the largest frame length that can be sent on a physical medium. The highest possible MTU value is the default value of 1500. The minimum value you should ever use is 552. The TCP Max segment size is the IP Maximum datagram size minus 40. The default IP Maximum Datagram Size is 576. The default TCP Maximum Segment Size is 536.
Statistics	Input/Output (I/O) information about the selected NIC port: • Packets In/Out – The number of packets in and out for this NIC port. • Errors In/Out – The number of errors in and out for this NIC port. • Collisions – The number of transmission collisions for this NIC port. • Clear Counters – Click to clear all counts on the Statistics tab: packets, errors, and collisions.
IP Aliases	The alias IP address applied to the selected NIC port. There can be up to nine aliases for single server systems, and up to four aliases for dual server systems. For dual server systems only, the value in this field can be the primary IP address of the corresponding port on the partner head, if necessary.
Partner IP Aliases	This field is available only for dual server systems. The primary IP address of the corresponding port on the partner head, if necessary. This field displays the IP addresses of the partner head that are reserved for backup purposes. These are the IP addresses that will be activated by the surviving head in the event of a failover.
	Click to move the IP alias value that you typed from the IP Aliases field into the list of available IP aliases.
	Click to remove the selected IP alias from the list of available IP aliases.

TABLE F-43 Fields and Elements on the Configure Network Adapters Panel *(Continued)*

Field	Description
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Create/Edit Port Bond Window

This window enables you to create or edit a bond between two or more network interface card (NIC) ports. This bond forms either a port aggregation bond or a high availability bond.

In a port aggregation bond, ports are combined to produce a higher bandwidth port. All NICs in this type bond must be of the same type of interface card (for example, Fast Ethernet with Fast Ethernet) and connect to the same subnet. In a high availability bond, ports are bonded to create port failover (NIC port redundancy). In this type of bond, NICs can be of different type of interface cards and be connected to different subnets.

The following table describes the fields and buttons in this window.

TABLE F-44 Fields and Elements on the Create/Edit Port Bond Window

Field	Description
IP Address	The Internet Protocol (IP) address designated for the port bond.
Subnet Mask	This field is available only if DHCP is disabled. The subnet netmask for the first NIC port added to the port bond.
Broadcast Address	The broadcast address associated with the bond. This broadcast address is used by the first NIC port (the primary port) listed in the NIC Ports in This Bond field.
Port Aggregation	The type of bond, also known as “channel bonding” or “trunking.” Lets you scale network I/O by joining NIC ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth. You must have a minimum of two available NIC ports for port bonding. **Note:** All NIC ports in an aggregation bond must be of the same type of interface card (e.g., Fast Ethernet with Fast Ethernet), be connected to the same subnet, and be connected to adjacent ports. For systems that use switches, the switch must support port (or channel) bonding.

TABLE F-44 Fields and Elements on the Create/Edit Port Bond Window *(Continued)*

Field	Description
High Availability	The type of port bond that provides NIC port failover. Multiple NIC ports can be bonded to a primary port as backup ports. When the primary port fails, the software automatically switches to the backup port at the top of the list of high-availability bonded ports. If that port also fails, the port next on the list is used, and so on. **Note:** NICs in a high-availability bond do not have to be the same type of interface card or be connected to the same subnet.
Available NIC Ports	The NIC ports available to be bonded.
	Click the top button to move the selected port from the Available NIC Ports box to the NIC Ports in This Bond box. Click the bottom button to move the selected port from the NIC Ports in This Bond box to the Available NIC Ports box.
NIC Ports in This Bond	The ports that already exist in this bond.
	If this is a high availability bond type, use the up and down arrow buttons to organize the order of the ports. The first port in the NIC Ports in This Bond list is the primary port. The second port is the first port to be used in case of a failover. The next port in the list is used in case the port before it also fails.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Set Gateway Address Panel

This panel enables you to specify the Sun StorageTek gateway address.

The following table describes the fields and buttons on this panel.

TABLE F-45 Fields and Elements on the Set Gateway Address Panel

Field	Description
Gateway	The gateway address for the system.

TABLE F-45 Fields and Elements on the Set Gateway Address Panel *(Continued)*

Field	Description
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Server Name Panel

This panel enables you to configure basic information about the Sun StorageTek server on your network.

The following table describes the fields and buttons on this panel.

TABLE F-46 Fields and Elements on the Set Server Name Panel

Field	Description
Server Name	The name by which the Sun StorageTek server is known on the network. The server name must begin with an alphabetical character (a–z, A–Z), and can include alphanumeric characters (a–z, A–Z, 0–9), dashes (-) and periods (.).
Company Name	The company name that will be included in any diagnostic email messages sent from this system.
Contact Name	The contact name that will be included in any diagnostic email messages sent from this system.
Contact Phone #	The phone number of the contact who will be included in any diagnostic email messages that are sent from this system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up DNS Panel

This panel enables you to set up the Domain Name Service (DNS) name service, which includes specifying the domain name and adding or removing a DNS server.

Note: If you are using DNS without Dynamic DNS, you must add the host name and Internet Protocol (IP) address of the system to the DNS database before entering values on this panel. If you are using Dynamic DNS, you do not need to manually update the DNS database. For more information, see your DNS documentation.

Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-47 Fields and Elements on the Set Up DNS Panel

Field	Description
Enable DNS	Select to enable DNS on the system.
Domain Name	The DNS domain name, which is the name by which the domain is known to the network.
Server	The IP address of a DNS server that you want to make available to the network.
Server List	Each existing DNS server that is available to the network. The DNS server at the top of the list is queried first for domain name resolution.
	Click to add the server entry that you typed from the Server field to the Server List menu.
	Click to remove the selected server from the Server List menu.
	Click to move the selected server up one position in the Server List menu.
	Click to move the selected server down one position in the Server List menu.
Enable Dynamic DNS	Select to enable a dynamic DNS client to add the system into the DNS namespace. If you enable dynamic DNS, you must also configure the Kerberos realm and Key Distribution Center (KDC) server on the "Configure Domains and Workgroups Panel" on page 397. When Dynamic DNS is enabled, non-secure dynamic updates automatically occur, if allowed by the DNS server.

TABLE F-47 Fields and Elements on the Set Up DNS Panel *(Continued)*

Field	Description
DynDNS User Name	The user name of a Windows 2000 user with whom the dynamic DNS client can authenticate to perform secure dynamic DNS updates. This user must reside within the Active Directory Service (ADS) domain and the Kerberos realm that is specified on the "Configure Domains and Workgroups Panel" on page 397. **Note:** If the domain administrator user name is displayed in this field but the ADS update fails, the domain administrator password must be changed (on the domain controller). This is only required for the administrator user, and the same password can be reused. For more information, see the Microsoft Support Services Web Site, Article Q248808.
DynDNS Password	The password of the DynDNS user. If you are updating this field, delete the entire password before entering a new one.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

View the Routing Table Panel

This panel enables you to view the following information about network routes.

TABLE F-48 Fields and Elements on the View the Routing Table Panel

Field	Description
Destination	The Internet Protocol (IP) address of the destination, which can refer either to a network or to a host. There must be one default route (such as, `0.0.0.0`), one loop-back route (such as, `127.0.0.1`), at least one network route, and at least one host route.
Gateway	The gateway address through which the packets travel to the destination.
Mask	The netmask for the destination network.
Interface	The type of interface that is used to send packets over the network.

TABLE F-48 Fields and Elements on the View the Routing Table Panel *(Continued)*

Field	Description
Flags	Indicators of the route status. Each type of status indication is represented by a number, in hexadecimal format. The following are some common flags and their meanings: • 0x1 – The route is usable. • 0x2 – The destination is a gateway. • 0x4 – The destination is a host entry. • 0x8 – The host or network is unreachable. • 0x10 – The destination was created dynamically. • 0x20 – The destination was modified dynamically. Some flags may be the sums of individual indicators. For example, 0x3 represents the route as being usable (0x1) and as being a gateway (0x2).

RAID Panels

This section describes the fields and elements on the RAID panels of the Web Administrator graphical user interface:

Add Hot Spare Window

This window enables you to designate a drive as a hot spare for the Sun StorageTek 5320 NAS Appliance or Cluster system. You do so by clicking on the drive image that you want.

The following table describes the drive images and buttons in this window.

TABLE F-49 Drive Images and Buttons in the Add Hot Spare Window

Drive	Indication
	The drive in this slot is available as a hot spare.
	The drive in this slot has been selected as a hot spare.
	No drive is present in this slot.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Add LUN Window

This window enables you to add a logical unit number (LUN) to the system configuration.

Note: To add a new LUN from this window, you must select the drives that will belong to the LUN. You do so by clicking each drive image displayed in the window. At least three drives must be selected. The drive images show the status of each drive, as described in the following table.

TABLE F-50 Add LUN Window Drive Status Indicators

Drive	Indication
	The drive in this slot is available for LUN membership.
	The drive in this slot has been selected for LUN membership.
	No drive is present in this slot.

The following table describes the fields and buttons in this window.

TABLE F-51 Fields and Elements on the Add LUN Window

Field	Description
New LUN Assignments	
RAID Level	The redundant array of independent disks (RAID) configuration.
Controller	The number of the controller to which you want to add a LUN.
Head Id	This field is available only for dual server systems. The unique identifier assigned to this server (head).
Create New Volume	Select to create a new volume for this LUN. The entire LUN will be used to create the volume. Type the name of the new volume in the field.
Grow Existing Volume	Select to use this LUN to add disk space to an existing volume (to create and attach a segment). Then choose the volume you are growing from the drop-down menu.
None	Select to create a new LUN without assigning it a name.
Apply	Click to save your changes.

TABLE F-51 Fields and Elements on the Add LUN Window *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Locate Drive Tray Window

This window enables you to physically locate and identify a drive tray in the storage array. Locating a drive tray from this window causes the appropriate indicator light on all drives in the drive tray to flash.

The following table describes the drive images and buttons in this window.

TABLE F-52 Images and Buttons on the Locate Drive Tray Window

Drive	Indication
	Click to search for the drive tray in the storage array.
	Click to locate the drive tray. The indicator light or lights on the selected drive tray or drives will flash.
	Click after locating the drive tray to stop the flashing of the indicator light or lights on the drive tray or drives.
Cancel	Click to close out of the window.

Locate Drive Window

This window enables you to physically locate and identify one or more drives in a drive tray by activating drive indicator lights.

The following table describes the drive images and buttons in this window.

TABLE F-53 Locate Drive Window Drive Status Indicators

Drive	Indication
	Click to search for this drive in the drive tray.
	Click to locate the drive. The indicator lights on the selected drive will flash.
	Click after locating the drive to stop the flashing of the indicator light on the drive.
Cancel	Click to close out of the window.

Manage RAID Panel

This panel enables you to manage your Sun StorageTek redundant array of independent disks (RAID) array.

The following table describes the fields and buttons on this panel.

TABLE F-54 Fields and Elements on the Manage RAID Panel

Field	Description
Legend	A key that describes what can be displayed in the graphical representation of the Sun StorageTek RAID array: • Black - The drive is not present in the slot. • Green - The drive is present in the slot and is functional. • Orange - The data is being copied from the hot spare drive. • Yellow - The LUN is being created. • Red - The drive has failed. • Pink - The drive was replaced.
Capacity	The total amount of space available for storage use on the selected LUN.

TABLE F-54 Fields and Elements on the Manage RAID Panel *(Continued)*

Field	Description
Status	The status of the drive in the LUN.
Raid Level	The RAID configuration.
Lun Owner	The user who owns the LUN.
Remove LUN	Click to remove the selected LUN from the Sun StorageTek RAID array.
Add LUN	This button is available only if at least three drives are available in the Sun StorageTek RAID array. Click to launch the Add LUN window. From this window, you can add a LUN to the Sun StorageTek RAID array.
Remove HS	Click to remove a hot spare from the Sun StorageTek RAID array.
Add HS	Click to launch the Add Hot Spare window. From this window, you can add a hot-spare to the Sun StorageTek RAID array.
Locate Drive	Click to locate a drive. Clicking this option causes the LCD indicator for the drive to flash.
Locate Drive Tray	Click to locate a drive tray. Clicking this option causes the LCD indicator for the drive tray to flash.

View Controller/Enclosure Information Panel

This panel enables you to view information about the controllers or enclosures in the system.

The following table describes the fields and buttons on this panel.

TABLE F-55 Fields and Elements on the View Controller/Enclosure Information Panel

Field	Description
Controller Information	A list of the controllers in the Sun StorageTek redundant array of independent disks (RAID) array.
Vendor	The name of the controller vendor.
Model	The model number of the controller.
Firmware Release	The release level of the controller firmware.
Enclosure Information	

TABLE F-55 Fields and Elements on the View Controller/Enclosure Information Panel

Field	Description
Tray IDs	A list of the tray IDs associated with the enclosure.
Vendor	The name of the enclosure vendor.
Model	The model number of the enclosure.
Firmware Release	The release level of the enclosure firmware.

View LUN Information Panel

This panel enables you to view the logical unit numbers (LUNs) in the system.

The following table describes the fields and buttons on this panel.

TABLE F-56 Fields and Elements on the View LUN Information Panel

Field	Description
LUNs	A list of the LUNs in your system.
Vendor	The name of the LUN vendor.
Product	The LUN product.
Product Revision	The revision of the LUN product.
Size	The size of the LUN.
ID Type	The type of identifier used by the LUN.
Vendor ID	The identifier of the LUN vendor.
Vendor Specific ID	The identifier specific to the vendor.
Vendor Specific ID Extension	The extension of the identifier that is specific to the vendor.

System Activity Panels

This section describes the fields and elements on the System Activity panels of the Web Administrator graphical user interface:

- "View Networking Activity Panel" on page 365
- "View System Activity Panel" on page 365

View Networking Activity Panel

This panel enables you to view the number of I/O requests per second for all Sun StorageTek clients.

The following table describes the fields and buttons on this panel.

TABLE F-57 Fields and Elements on the View Networking Activity Panel

Field	Description
Clients	The Internet Protocol (IP) address of the Sun StorageTek client.
Requests	A number of I/O request, per second.

View System Activity Panel

This panel enables you to view the I/O requests per second between the system and the peripheral devices with which it communicates. The following are the peripheral devices that can be displayed on this panel:

- CPU – System central processing unit (CPU)
- Memory – System random access memory (RAM)
- Port Aggregation x – Port aggregation x
- Controller x – RAID controller x
- dac1d0xx – Logical unit numbers (LUNs) xx
- PORTx – Network interface card (NIC) port x
- Host Adapter x – Internet Small Computer Systems Interface (iSCSI) host adapter x (for tape backup device)

Note: The names and number of devices being monitored will vary, depending on the Sun StorageTek hardware configuration.

The following table describes the fields and buttons on this panel.

TABLE F-58 Fields and Elements on the View System Activity Panel

Field	Description
Device	The peripheral device that communicates with the system.

TABLE F-58 Fields and Elements on the View System Activity Panel *(Continued)*

Field	Description
Load	The current load of the device, in terms of I/O requests per second.
Peak	The peak load of the device.

System Backup Panels

This section describes the fields and elements in the System Backup panel of the Web Administrator.

Set Up NDMP Panel

This panel enables you to set up the architecture for the Network Data Management Protocol (NDMP), which is an open protocol for network-based backup. NDMP architecture enables vendors of network attached storage to ship NDMP-compliant servers that can be used with any NDMP-compliant backup administration application. Local backup is not available when using NDMP.

Note: For you to use NDMP, the backup administration application must be configured for logon with the user name `administrator` and with the password that is used by the console (command-line interface) administrator.

Note: For volumes to be backed up by NDMP, checkpoints must be enabled. For more information, see "Creating File Checkpoints" on page 163.

The following table describes the fields and buttons on this panel.

TABLE F-59 Fields and Elements on the Set Up NDMP Panel

Field	Description
NDMP NIC	The adapters, bonds, and Internet Protocol (IP) addresses in the system. The selected adapter or bond is used for NDMP: • Adapter - The name of the NDMP NIC adapter. • IP Address - The IP address of the adapter.
Gateway	The gateway address for the selected NDMP NIC. If the NDMP backup tape device is located on another network, be sure to select the NIC that connects to the correct gateway.

TABLE F-59 Fields and Elements on the Set Up NDMP Panel *(Continued)*

Field	Description
NDMP Log	The full path for NDMP logging. This path specifies the directory where the NDMP log file and other temporary data files used by NDMP are stored. This path needs to be on a valid system volume, and the volume must be writable in order for NDMP to work.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

System Manager Panels

This section describes the fields and elements in the System Manager panels of the Web Administrator graphical user interface:

- "Edit NFS Export Window" on page 367
- "Server Properties Window" on page 368
- "Volume Properties Window" on page 368

Edit NFS Export Window

This window enables you to update the access permission for the selected NFS export and update the mapping of the UID for root users.

The following table describes the fields and buttons in this window.

TABLE 12-3 Fields and Elements on the Edit NFS Export Window

Field	Description
Hosts	The hosts to which the selected export is defined.
Access	
Read/Write	Select to assign read/write access privileges to the export.
Read/Only	Select to assign read/only access privileges to the export.
No Access	Select to assign no access privileges to the export.
Map Root User	

TABLE 12-3 Fields and Elements on the Edit NFS Export Window *(Continued)*

Field	Description
Anonymous User	Select to map the user ID (UID) of root users (users with a UID of `0`) to the user ID of the anonymous user (the user `nobody`).
Root User	Select to have root users use the UID of root (`uid=0`).
Map to UID	Select to map the UID of root users to the UID that you specify in the field.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Server Properties Window

This window enables you to view the basic properties of the Sun StorageTek server. To open this window, right-click the volume name under System Manager.

The following table describes the fields and buttons in this window.

TABLE F-60 Fields and Elements on the Server Properties Window

Field	Description
Name	The name of the server.
Model	The model number of the server.
Serial #	The serial number of the server.
OS Version	The operating system version being used by the server.
Cancel	Click to close out of the window.

Volume Properties Window

This window enables you to view the properties of the selected volume. To open this window, right-click System Manager and select Properties.

The following table describes the fields and buttons on this window.

TABLE F-61 Fields and Elements on the Edit Volume Properties Window

Field	Description
Label	The label of the volume.
Checkpoints	Whether checkpoints are enabled for the volume.
Quotas	Whether quotas are enabled for the volume.
Capacity	The total amount of storage space on the volume. A graphical representation of storage usage is displayed: • Used – The amount of space used on the volume. • Free – The amount of space available for storage use on the volume.
Partitions	
Legend	Indicators in the graphical depiction of the selected LUN configuration: • Orange – Indicates the primary partition on the volume. • Light Blue – Indicates the segmented partition on the volume. • Green – Indicates the mirror on the volume. • Blue – Indicates that the DOS read-only attribute is applied to the volume. This DOS read-only attribute is only used on the flash disk for the system volume. • White – Indicates the free space on the volume.
Enable Attic	Click to temporarily save deleted files in the `.attic$` directory located at the root of the volume. By default, this option is enabled. In rare cases on very busy file systems, the `.attic$` directory can be filled faster than it processes deletes, leading to a lack of free space and slow performance. In such a case, you should disable the `.attic$` directory by deselecting this.
Lun	The name of the LUN on which the selected volume resides.
Partition	The LUN partition on which the volume resides.
Use (%)	The percentage of space used on the volume.
Type	The type of volume, such as primary or segmented.
Free (MB)	The amount of space available on the volume for storage use.
Capacity (MB)	The total amount of space on the volume for storage use.
Cancel	Click to close out of the window.

System Operations Panels

This section describes the fields and elements on the System Operations panels of the Web Administrator graphical user interface:

Activate Options Panel

This panel enables you to view existing licenses on the system, add licenses to and remove licenses from the system, and enable temporary licenses on the system.

The following table describes the fields and buttons on this panel.

TABLE F-62 Fields and Elements on the Activate Options Panel

Field	Description
Module	The name of the licensable module.
State	Whether the license is valid.
Status	Whether the license is active.
Origination	The date on which the license became active, in YYYYMMDD format. If this field displays a value of 00000000, the license is immediately active. **Note:** This date is validated against the secure clock.
Expiration	The date on which the license expires, in YYYYMMDD format. If this field displays the value of 00000000, the license never expires. **Note:** This date is validated against the secure clock.

TABLE F-62 Fields and Elements on the Activate Options Panel *(Continued)*

Field	Description
Key	The unique license key assigned to the license.
Add	Click to launch the Add License window. From this window, you can add a new license to the Sun StorageTek server. **Note:** Licenses cannot be added to the system until the secure clock is initialized. The secure clock is initialized the first time you set the date and time on the system. For more information, see "Setting the Time and Date Manually" on page 64. Make sure you set the time accurately, as the secure clock can only be set once.After you set the initial time and date, the license is not affected by additional changes to the time and date.
Remove	Click to delete the selected license from the system.
Temporary Licenses	Click to launch the Enable Temporary Licenses window. From this window, you can activate any available temporary licenses on the system.
Import	Click to read license information from a file (the default system license path is searched) and import the information into the system.

Add License Window

This window enables you to add a license with the specified parameters to the system.

The following table describes the fields and elements in this window.

TABLE F-63 Fields and Elements on the Add License Window

Field	Description
Module	The licensable module name.
Origination	The date on which the license becomes active, at 0000:00 hours.
Expiration	The date on which the license expires, at 2359:59 hours. **Note:** Dates are specified in the format YYYYMMDD. The special date string 00000000 indicates that there is no restriction. If this string is used as the origination date, the license is active immediately; if it is used as the expiration date, the license never expires.
Key	The license key, which must be in UUID format: XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXXXXXX.

TABLE F-63 Fields and Elements on the Add License Window *(Continued)*

Field	Description
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Assign Language Panel

This panel enables you to choose the language that is displayed in the Web Administrator application. The Web Administrator application supports Unicode, officially known as the Unicode Worldwide Character Standard. This is a system for the interchange and display of international and classical languages.

Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel in the wizard.

The following table describes the fields and buttons on this panel.

TABLE F-64 Fields and Elements on the Assign Language Panel

Field	Description
Codepage	Select a language codepage for the Sun StorageTek server.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Enable Temporary Licenses Window

This window lets you enable the available temporary licenses for the system.

The following table describes the fields and elements in this window.

TABLE F-65 Fields and Elements on the Enable Temporary Licenses Window

Field	Description
Module	The licensable module name.

TABLE F-65 Fields and Elements on the Enable Temporary Licenses Window *(Continued)*

Field	Description
Duration	The number of days for which this temporary license will be enabled.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Import Licenses Window

This window enables you to import a license from a file.

Note: If you choose to copy and paste, or manually enter the license information, please be sure you do not accidentally insert any line breaks within the license information. Otherwise, the lines will not be recognized as valid entries.

The following table describes the fields and elements in this window.

TABLE F-66 Fields and Elements on the Enable Temporary Licenses Window

Field	Description
Import License Field	The license information of the license you want to import.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.
Browse	Click to import the license from a file.

Set Administrator Password Panel

This panel enables you to set the system administrator password.

The following table describes the fields and buttons on this panel.

TABLE F-67 Fields and Elements on the Set Administrator Password Panel

Field	Description
Old	The existing system administrator password. If there is no password, leave this field is blank.
New	The new system administrator password. The password must be at least one and no more than 21 characters long. If you want to disable the administrator password, leave this field blank.
Confirm	The new system administrator password, typed a second time.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Remote Access Panel

This panel enables you to set up network services that are used to remotely administer a Sun StorageTek filer. The following are the available network services:

- Telnet
- Remote Login
- Remote Shell
- Secure Shell, Web Admin (over Hypertext Transfer Protocol (HTTP))
- Secure Web Admin (over Secure Hypertext Transfer Protocol (HTTPS))

The following table describes the fields and buttons on this panel.

TABLE F-68 Fields and Elements on the Set Remote Access Panel

Field	Description
Secure Mode	Click to enable only those protocols that are deemed to be secure. This disables all other services. The following are the secure protocols: • Secure Web Admin, which uses the Secure Socket Layer (SSL) over HTTP • Secure Shell (ssh)
Service	The existing services that are available to the Sun StorageTek filer.

TABLE F-68 Fields and Elements on the Set Remote Access Panel *(Continued)*

Field	Description
Enabled	Click to enable the corresponding service for remote access to the Sun StorageTek filer.
Comment	A line of text that describes the service.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Time and Date Panel

This panel enables you to set the Sun StorageTek server time and date.

The following table describes the fields, elements, and buttons on this panel.

TABLE F-69 Fields and Elements on the Set Time and Date Panel

Field	Description
Calendar	The current year, month, and day, in graphical format. To change the current year or month, choose the options that you want from the appropriate drop-down menus on the calendar. To update the day, click the calendar itself.
Clock	The current time, in graphical format. To change the current time, choose a new time from the drop-down menus located immediately above the clock. These drop-down menus display the time in military format (for example, 1:30 is displayed as 13:30).
Time Zone Drop-Down Menu	The current time zone of the Sun StorageTek server. To change the time zone, choose a new time zone from the drop-down menu.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Time Synchronization Panel

This panel enables you to synchronize the Sun StorageTek server time to either the Network Time Protocol (NTP) protocol or an RDATE server. NTP is an Internet Protocol used to synchronize the clocks of computers to a reference time source, such as a radio, satellite receiver or modem. Typical NTP configurations use multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

The RDATE time protocol provides a site-independent date and time. It is a protocol that can retrieve the time from another machine on your network. RDATE servers are commonly present on UNIX systems.

The following table describes the fields and buttons on this panel.

TABLE F-70 Fields and Elements on the Set Up Time Synchronization Panel

Field	Description
Manual Synchronization	Select to use neither NTP nor RDATE time synchronization.

TABLE F-70 Fields and Elements on the Set Up Time Synchronization Panel *(Continued)*

Field	Description
NTP Synchronization	Select to use NTP synchronization, which requires that you have at least one NTP server on the network. The following options are specific to NTP synchronization: • Enable Server 1, Enable Server 2 - Click either checkbox to enable that NTP server. Up to two NTP servers can be enabled. • NTP Server –The name or Internet Protocol (IP) address of the NTP server that the Sun StorageTek server will poll for the current time. • Auth Type – Choose the type of authentication to be used between the Sun StorageTek server and the NTP server. Authentication support enables the Sun StorageTek server to use a key and key identifier to verify that the NTP server is known and trusted. The NTP server and the Sun StorageTek server must agree on the key and key identifier to authenticate their messages. • Key ID – The key identifier that is associated with the private key from the `ntp.` key file that will be used with this NTP server. This field needs a value only if Symmetric Key was selected in the Auth Type field. The valid range for the Key ID value is 1 to 65534. **Note:** The `ntp.` key file must be copied to the `\etc` directory before symmetric key authentication is used. • Min Poll Rate – The minimum polling rate for NTP messages. This value to the power of 2 indicates the minimum number of seconds of the polling interval. For example, a value of 6 represents 36 seconds. The valid range for this field is 4 to 17. The default value of 6 is sufficient for most installations. • Max Poll Rate – The maximum polling rate for NTP messages. This value to the power of 2 indicates the maximum number of seconds of the polling interval. For example, a value of 4 represents 16 seconds. The valid range for this field is 4 to 17 but it must be larger than the minimum polling interval value. The default value of 10 is sufficient for most installations. • Enable Broadcast Client – Click to have the Sun StorageTek server respond to NTP server broadcast messages received on any interface. This is intended for configurations involving one or more NTP servers with a large number of clients that require time synchronization from those servers. • Require Broadcast Server Authentication – Click to require the NTP client to verify that a server that has broadcast messages to the Sun StorageTek server is a known and trusted server.

TABLE F-70 Fields and Elements on the Set Up Time Synchronization Panel *(Continued)*

Field	Description
RDATE Synchronization	Select to use the RDATE server time synchronization with the Sun StorageTek server. The following options are specific to RDATE server synchronization: • RDATE Server – The name or IP address of the RDATE server. • Tolerance – The maximum tolerance between the time on the Sun StorageTek server and the time received from the RDATE server, between 0 and 3600 seconds. If the Sun StorageTek server time is later or earlier than the RDATE server time by less than this number of seconds, the Sun StorageTek server time will be synchronized with RDATE server time. If there is a larger discrepancy, the Sun StorageTek server time will not be automatically synchronized with the RDATE server. This validation occurs every day at 11:45 PM.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Shut Down the Server Panel

This panel enables you to halt or reboot the Sun StorageTek server.

The following table describes the fields and buttons on this panel.

TABLE F-71 Fields and Elements on the Shut Down the Server Panel

Field	Description
None	Click to perform neither a shutdown nor a reboot of the server, or servers.
Halt both heads	This field is available only for dual server (cluster) systems. Click to shut down both servers in a cluster configuration. Check to be sure both servers in the cluster are in the NORMAL state. To restart, you must manually power on the servers.
Reboot both heads	This field is available only for dual server (cluster) systems. Click to shut down and restart both servers in a cluster configuration.
Halt	This field is available for single server systems. Click to shut down the server. To restart, you must manually power on the server.
Reboot	This field is available for single server systems. Click to shut down and restart the server.

TABLE F-71 Fields and Elements on the Shut Down the Server Panel *(Continued)*

Field	Description
Reboot Previous Version *version-number*	Select to shut down and restart the server, or servers, with an earlier version of the software. Use this option if you upgraded the software but encountered a problem. The server, or servers, is restarted with the last software used before the upgrade. In a cluster configuration, you must perform this action on each head in the cluster. **Note:** It is recommended that you check with Technical Support before choosing this option.
Halt this head	This field is available only for dual server systems. Click to shut down this server (the one to which you are currently logged on). The other server remains online. To restart, you must manually power on the server.
Reboot this head	This field is available only for dual server systems. Click to shut down and restart this server (the one to which you are currently logged on). The other server remains online.
Apply	Click to execute a server shutdown or reboot.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel. **Note:** You cannot cancel a server shut down or reboot after the shutdown or reboot has been initiated. Clicking Cancel only removes the entries you have typed on the panel.

Update Software Panel

This panel displays the current Sun StorageTek 5320 NAS Appliance software version on the Sun StorageTek server and enables you to update the server with later versions of the software. You can update the server by downloading software from the Sun Microsystems web site and uploading it from your floppy or CD-ROM drive.

The following table describes the fields and buttons on this panel.

TABLE F-72 Fields and Elements on the Update Software Panel

Field	Description
The Current OS Version	The current version of the Sun StorageTek 5320 NAS Appliance software on the Sun StorageTek server.

TABLE F-72 Fields and Elements on the Update Software Panel *(Continued)*

Field	Description
Update Server from a File	
Path	The full path to the software file on your workstation. This file, which you can obtain from the Sun Microsystems web site, can be used to update the Sun StorageTek 5320 NAS Appliance software version on the Sun StorageTek server.
Browse	Click to locate the software file you want to install from your workstation.
Update	Click to execute the software upload from the file you have selected. When you have completed the upload process, the system prompts you to reboot the server. Click Yes to reboot, or No to continue without rebooting. The software update will not occur until you have rebooted the system.

UNIX Configuration Panels

This section describes the fields and elements on the UNIX Configuration panels of the Web Administrator graphical user interface:

Add/Edit Comment Window

This window enables you to add or edit a comment about a Network File System (NFS) export, depending on how you accessed the window (by clicking the Add or Edit icon on the “Configure Exports Panel” on page 384).

The following table describes the fields and buttons in this window.

TABLE F-73 Fields and Elements on the Add/Edit Comment Window

Field	Description
Add Comment	A line of text, up to 80 characters in length, that relates to an NFS export. You can start the comment text with the # character, or remove the # character to add a blank line.
Ok	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add/Edit Host Window

This window enables you to add or edit a host, depending on whether you accessed the window by clicking Add or Edit.

Caution: Exercise caution when granting trusted status to hosts. Trusted hosts have root access to the Sun StorageTek file system, and can thus perform administrative functions in that file system.

The following table describes the fields and buttons in this window.

TABLE F-74 Fields and Elements on the Add/Edit Host Window

Field	Description
Host Name	The name of the host. The host name can include alphanumeric (a–z, A–Z, 0–9), dashes (-), and periods (.). The first character must be alphabetical (a–z or A–Z).
IP Address	The Internet Protocol (IP) address of the host.
Trusted	Whether the host is trusted. A trusted host has root access to the Sun StorageTek file system.

TABLE F-74 Fields and Elements on the Add/Edit Host Window *(Continued)*

Field	Description
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit NFS Export Window

You can add and edit Network File System (NFS) exports from by clicking the Add or Edit icon on the "Configure Exports Panel" on page 384 or by right-clicking a System Manager item and choosing the appropriate Add Export menu option.

You can only add NFS exports to whole volumes.

The following table describes the fields and buttons in this window.

TABLE F-75 Fields and Elements on the Add/Edit NFS Export Window

Field	Description
Volume	This field is available only if you clicked Add on the Configure Exports panel. Choose the volume for which you are adding or editing an NFS export. You can only choose whole volumes.
Path	This field is available only if you clicked Add on the Configure Exports panel. The directory for which you want to grant UNIX NFS host access. Leaving this field blank exports the root directory of the volume.
Full Path	The full path to the exported directory on the volume.
Access	
Read/Write	Select to grant the specified hosts Read/Write permissions on the selected volume.
Read/Only	Select to grant the specified hosts Read/Only permissions on the selected volume.
No Access	Select to grant the specified hosts No Access permissions on the selected volume.
Map Root User	
Anonymous User	Select to map the user ID of root users to the user ID of anonymous users on this export.

TABLE F-75 Fields and Elements on the Add/Edit NFS Export Window *(Continued)*

Field	Description
Root User	Select to map the user ID of root users to the user ID of root (UID= 0) on this export.
Map to UID	Select to assign a specific user ID to be used for root users on this export, and type the user ID.
Hosts	
Host Netgroups	This field is editable only in Add mode. Select to define the NFS export for a net group. From the drop-down menu, choose the net group to which you want to assign the export.
Host Group	This field is editable only in Add mode. Select to define the NFS export for a host group. From the drop-down menu, choose general (all hosts), trusted (all trusted hosts), or a user-defined host group.
Known Host	This field is editable only in Add mode. Select to define the export to a host that was added on the Set Up Hosts panel. From the drop-down menu, choose the host to which you want to assign the export.
Other Host	This field is editable only in Add mode. Select to define the export to an individual host that you have not added through the Set Up Hosts panel. In the field to the right, type the name of the host.
Ok	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add Hostgroup Window

This window enables you to add a host group to the configuration.

The following table describes the fields and buttons in this window.

TABLE F-76 Fields and Elements on the Add Hostgroup Window

Field	Description
Add Hostgroup	The name of the host group that you want to add. The name can include alphanumeric (a–z, A–Z, 0–9), dashes (-), and periods (.). The first character must be alphabetical (a–z or A–Z only).
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add Hostgroup Member Window

This window enables you to add members to the selected host group.

The following table describes the fields and buttons in this window.

TABLE F-77 Fields and Elements on the Add Hostgroup Member Window

Field	Description
Host Netgroups	Select this option and choose a Net group that is defined on an external NIS server to add as a member.
Host Group	Select this option and choose a host group to add as a member.
Known Host	Choose a host that you have manually added on the Set Up Hosts panel or that exists on an external NIS server to add as a member.
Other Host	Type a host that is not available from the Set Up Hosts panel to add as a member.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Configure Exports Panel

This panel enables you to specify access privileges for UNIX users to specified volumes. The table on this panel shows the current Network File System (NFS) export information, including the accessible directories, host name, and access level (read/write or read/only) for each export.

Any host name beginning with @ represents a group of hosts. For instance, a host name of `@general` represents a predefined host group that includes all hosts. A host name of `@trusted` represents a predefined host group that includes trusted hosts.

Any host name beginning with & represents a host net group. For example, `&group1` represents `netgroup, group1`.

The following table describes the fields and buttons on this panel.

TABLE F-78 Fields and Elements on the Configure Exports Panel

Field	Description
Full Path	The full path to the directory for which you want to grant UNIX NFS access privileges.
Host	The name of the host, or hosts, that have access privileges on the volume.
Access	The level of access the host has on the volume. Access can be read/write (R/W) or read/only (R/O).
Map Root User	The method for mapping the user ID for root users. For more information, see “Creating Exports” on page 118.
	Click to launch the Add NFS Export window. From this window, you can add a new NFS export to the configuration.
	Click to launch the Add Comment window. From this window, you can add a comment to the Configure Exports table.
	Click to launch the Edit NFS Export window or the Edit Comment window. From this window, you can edit the selected NFS export or comment.
	Click to delete the selected NFS export or comment from the table.
	Click to move the selected NFS export or comment to the top of the table.
	Click to move the selected NFS export or comment up one listing in the table.
	Click to move the selected NFS export or comment down one listing in the table.
	Click to move the selected NFS export or comment to the bottom of the table.

Configure Name Services Panel

This panel enables you to choose the order in which name services (NS) are used for group, Net group, host, and user lookup functions. The NS lookup order controls the sequence in which the name services are searched to resolve a query. The supported name services are: NIS, NIS+, NSSLDAP, DNS, and Local. Before you can use a name service for name resolution, the service must be enabled.

The following table describes the fields and buttons on this panel.

TABLE F-79 Fields and Elements on the Configure Name Services Panel

Field	Description
Groups Order	Click to display the name services that are available to be searched for group lookup functions.
Netgroup Order	Click to display the name services that are available to be searched for Net group lookup functions.
Hosts Order	Click to display the name services that are available to be searched for user lookup functions.
Users Order	Click to display the name services that are available to be searched for host lookup functions.
Services Not Selected	The available name services that will not be used for lookup functions.
	Click the top button to move the selected name service from the Services Not Selected menu to the Services Selected menu. Click the bottom button to move the selected name service from the Services Selected menu to the Services Not Selected menu.
Services Selected	The available services, in sequential order, that will be used for lookup functions. These services must be enabled.
	These buttons are available only if there is more than one name service listed in the Services Selected menu. Click the top button to move the selected name service up in the list. Click the bottom button to move the selected name service down in the list.
Apply	Click to save your changes.

TABLE F-79 Fields and Elements on the Configure Name Services Panel *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Remove NFS Export Window

This window enables you to delete a network file system (NFS) export from the configuration.

The following table describes the fields and buttons on this panel.

TABLE F-80 Fields and Elements on the Configure Exports Panel

Field	Description
Host	The name of the host, or hosts, that have access privileges on the volume.
Access	The level of access the host has on the volume. Access can be read/write (R/W) or read/only (R/O).
Apply	Click to delete the selected NFS export from the configuration.
Cancel	Click to exit out of the window without saving any changes.

Set Up FTP Panel

This panel enables you to set up File Transfer Protocol (FTP) service on the system and to define user access to the system by using FTP.

The following table describes the fields and buttons on this panel.

TABLE F-81 Fields and Elements on the Set Up FTP Panel

Field	Description
Enable FTP	Select to enable FTP on the system. If the FTP service is enabled, the FTP server accepts incoming connection requests.

TABLE F-81 Fields and Elements on the Set Up FTP Panel *(Continued)*

Field	Description
Allow Guest Access	Select to enable access to the FTP server by anonymous users.
Allow User Access	Select to enable access to the FTP server by all users. If this checkbox is deselected, only `admin` and `root` users can access the FTP server.
Allow Admin Access	Select to enable access to the FTP server by all `root` users. A user is considered a root user if he or she is the special `admin` Sun StorageTek user or if his or her user identifier (UID) is equal to 0.
Enable Logging	Select to enable FTP logging.
Log File Name	This field is available only if logging is enabled. The name of the FTP log file.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Hostgroups Panel

This panel enables you to monitor and manage the host groups database. Groups and group members can be added to or deleted from this database. Host groups are used to define a collection of hosts that can be used in Network File System (NFS) exports. Groups consist of predefined system groups and user-defined groups. The two predefined groups are the Trusted and iso8859 groups.

The following table describes the fields and buttons on this panel.

TABLE F-82 Fields and Elements on the Set Up Hostgroups Panel

Field	Description
Groups	Choose a group from the drop-down menu to display its members in the Group Members menu.
	Click to launch either the Add Hostgroup or the Add Hostgroup Member window, depending on whether you click this button in the Groups or the Group Members section of the panel. For more information about adding new host groups or host group members, see “Adding a Host Group” on page 90 or “Adding a Member to a Host Group” on page 91.

TABLE F-82 Fields and Elements on the Set Up Hostgroups Panel *(Continued)*

Field	Description
	Click to delete the selected host group or selected host group member, depending on whether you click this button in the Groups or the Group Members section of the panel.
Group Members	The members of the selected host group.

Set Up Hosts Panel

This panel enables you to add, edit, or remove host entries from the system host file.

Caution: Exercise caution in granting trusted status to hosts. Trusted hosts have root access to the Sun StorageTek file system and can therefore perform administrative functions in that file system.

The following table describes the fields and buttons on this panel.

TABLE F-83 Fields and Elements on the Set Up Hosts Panel

Field	Description
Host Name	The name by which the host is known on the system. Use upper- or lower-case alphabetical characters, numbers, periods (“.”) or a hyphen (“-”) only. The first character must be an alphabetic character.
Trusted	Whether the host is trusted. A trusted host has root access to the Sun StorageTek file system.
IP Address	The Internet Protocol (IP) address of the host.
Add	Click to launch the Add Host window. From this window, you can add a new host to the system host file.
Remove	Click to delete the host from the system host file.
Edit	Click to launch the Edit Host window. From this window, you can edit information about the selected host.

Set Up NIS Panel

This panel enables you to set up the Network Information Service (NIS) name service for the system. If you are running a pure Windows network, you do not need to set up NIS.

Note: If you are accessing this panel through the configuration wizard, make your changes and click Next to proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-84 Fields and Elements on the Set Up NIS Panel

Field	Description
Enable NIS	Select to enable NIS, which configures the system to import the NIS database for host, user, and group information.
Domain Name	The name of the domain to be used for NIS services.
Server	The Internet Protocol (IP) address or name of the NIS server from which the NIS database is imported.
Check Rate	The frequency, in minutes, that NIS information is refreshed. The default is 5 minutes.
Use Broadcast	Select to automatically acquire the NIS server name or IP address. This option is useful if you know the NIS domain name but not the NIS server name.
Update Hosts	Select to download the host information from the NIS server to the system.
Update Users	Select to download the user information from the NIS server to the system.
Update Groups	Select to download the group information from the NIS server to the system.
Update Netgroups	Select to download the Net group information from the NIS server to the system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up NIS+ Panel

This panel enables you to set up the Network Information Service Plus (NIS+) name service for the system. If you are running a pure Windows network, you do not need to set up NIS+.

Before enabling NIS+ on this panel, you must perform configuration steps on your NIS+ server. For more information, see "Setting Up NIS+" on page 30.

The following table describes the fields and buttons on this panel.

TABLE F-85 Fields and Elements on the Set Up NIS+ Panel

Field	Description
Enable NIS+	Select to enable NIS+ on the system.
Home Domain Server	The name or Internet Protocol (IP) address of the NIS+ home domain server.
NIS+ Domain	The name of the NIS+ home domain.
Secure RPC Password	The password used by the system to enable communication with the NIS+ server.
Search Path	The domains that NIS+ searches through when looking for information. This field can be blank if you want NIS+ to search only the home domain and its parents. For example, if the NIS+ domain is `eng.sun.com` and the Search Path field is blank, the system first searches `eng.sun.com` then `sun.com`, and so on, when resolving names. Conversely, if the Search Path value is `sun.com`., the system searches only the domain `sun.com` when resolving names.
Use Broadcast	Select to automatically acquire the NIS+ server name or IP address. This option is useful if you know the NIS+ home domain name but not the NIS+ server name.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up NSSLDAP Panel

This panel enables you to set up Name Service Switch Lightweight Data Access Protocol (NSSLDAP), which is a UNIX service that enables user account authentication.

The following table describes the fields and buttons on this panel.

TABLE F-86 Fields and Elements on the Set Up NSSLDAP Panel

Field	Description
Enable NSSLDAP	Select to enable NSSLDAP for the system.
Domain (DN)	The Lightweight Data Access Protocol (LDAP) domain name, in domain name (DN) or LDAP format.
Password	The bind password on the NSSLDAP server.
Server	The Internet Protocol (IP) address of the NSSLDAP server.
Proxy (DN)	The NSSLDAP proxy (entryDN).
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Windows Configuration Panels

This section describes the fields and elements on the Windows Configuration panels of the Web Administrator graphical user interface:

- "Set Up WINS Panel" on page 404
- "System Status Panel" on page 405

Add/Edit Group Window

This window enables you to add or edit a group, depending on whether you accessed the window by clicking Add Group or Edit Group.

The following table describes the fields and buttons in this window.

TABLE F-87 Fields and Buttons on the Add/Edit Group Window

Field	Description
Group	The name of the share.
Comment	(Optional) A brief line of text that describes the group.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit Share Window

You can add and edit shares on the Configure Shares panel or by right-clicking a System Manager item in the navigation pane and choosing the appropriate option from the menu.

This window enables you to add or edit a static Server Message Block (SMB) share, depending on whether you accessed the window in Add or Edit mode.

The following table describes the fields and buttons in this window.

TABLE F-88 Fields and Buttons on the Add/Edit Share Window

Field	Description
Old Share Name	This field is available only if you are in Edit mode. The current name of the share.

TABLE F-88 Fields and Buttons on the Add/Edit Share Window *(Continued)*

Field	Description
Share Name	The name of the share. This is the name that users will see on the network. The following characters are not supported in the share name: = | : ; \ " ? < > * /
Comment	(Optional) A brief line of text that describes the share. You can enter up to 60 alphanumeric characters.
Path	This field is not available if you clicked Add on the Configure Shares panel to access the window. This field is editable only if you clicked Edit on the Configure Shares panel. The full path of the share on the selected volume.
Mac Extensions	Click the Desktop DB Calls checkbox to allow the system to access and set Macintosh desktop database information. Enabling this option speeds up Macintosh client file access on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System and allows non-Macintosh clients to access Macintosh files on the system.
Volume Name	This field is available only if you clicked Add on the Configure Shares panel to access the window. Choose the volume that you want to share from the drop-down menu.
Directory	This field is available only if you clicked Add on the Configure Shares panel. An existing directory path. You cannot create a directory in this field. Note that directory names are case-sensitive. Do not leave this field blank. **Note:** A root-level share is created if the directory is omitted.
Container	This field is available only if you have enabled Active Directory Service (ADS) for the share on the "Configure Domains and Workgroups Panel" on page 397. (Optional) The ADS container in which the share is to be published. This is the ADS path location for the share in, Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation. Objects, such as users and shares, are located within Active Directory domains according to a hierarchical path, which includes each level of "container" objects. **Note:** Type the path in terms of the `cn` (common name) folder or `ou` (organizational unit) of the share. The `cn` containers are default folders in the `root` folder. All other containers are `ou` folders. For example, if the share will reside in a `shares` organizational folder within an organizational parent folder called `accounting`, you would type the following: **`ou=shares,ou=accounting`** Do not include the domain name in the path.

TABLE F-88 Fields and Buttons on the Add/Edit Share Window *(Continued)*

Field	Description
User ID	This field is available only if Windows Workgroup mode (not NT Domain mode) is enabled on the "Configure Domains and Workgroups Panel" on page 397. The user identification of the user accessing the specified directory through this share. The default value for this field is `0` (zero), which is the value of the UNIX root user. However, use caution in assigning this value. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in that share.
Group ID	This field is available only if Windows Workgroup mode (not NT Domain mode) is enabled on the "Configure Domains and Workgroups Panel" on page 397. The group identification of the user accessing the specified directory through this share. The default value for this field is `0` (zero), which is the value of the UNIX root user. However, use caution in assigning this value. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in that share.
Umask	The access permission parameter (a three-digit number) for the share. For detailed information about access permissions for shares, see "About Share Access Permissions" on page 105.
R/W Password	The password for Windows Workgroup users who will have read/write access to the directories specified for this share.
Confirm R/W Password	A field used to confirm the password you entered in the R/W Password field.
R/O Password	The password for Windows Workgroup users who will have read-only access to the share.
Confirm R/O Password	A field used to confirm the password you entered in the R/O Password field.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit SMB/CIFS User or Group Map Window

This window enables you to add or edit the SMB/CIFS user or group map, depending on whether you accessed the window by clicking Add or Edit on the "Configure Maps Panel" on page 401.

The following table describes the fields and buttons in this window.

TABLE F-89 Fields and Buttons on the Add/Edit SMB/CIFS User or Group Map Window

Field	Description
NT Group	
Account	The NT account name of the user or group you want to map.
RID	The relative identifier that uniquely identifies the NT user or group within the NT domain.
Unix Group	
Name	The UNIX user or group name to which you want to map the specified NT user or group.
ID	The identifier that uniquely identifies the UNIX user or group within the UNIX domain.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Configure Autohome Panel

This panel enables you to configure autohome shares. Autohome shares are temporary shares that are created when a user logs in to the system and then removed when the user logs out. For more information, see "About Autohome Shares" on page 110.

The following table describes the fields and buttons on this panel.

TABLE F-90 Fields and Buttons on the Configure Autohome Panel

Field	Description
Enable Autohome	Select to enable the autohome feature.
Autohome Path	The base directory path for temporary shares. For example, if a user's home directory is `/vol1/home/tom`, then the autohome path value is `/vol1/home`. For more information about how to specify valid values in this field, see "Enabling Autohome Shares" on page 111.

TABLE F-90 Fields and Buttons on the Configure Autohome Panel *(Continued)*

Field	Description
ADS Container	This field is available only if you have enabled ADS for the system on the "Configure Domains and Workgroups Panel" on page 397. The Active Directory Service (ADS) container in which the temporary shares can be published. For more information about how to specify valid values in this field, see "Enabling Autohome Shares" on page 111.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Domains and Workgroups Panel

This panel enables you to configure Windows networking for either a Windows NT Domain or a Workgroup security model.

Note: If the security model changes between the Windows Workgroup and NT Domain model, a confirmation message prompts you to confirm an automatic server reboot. Click Yes to reboot the system.

The following table describes the fields and buttons on this panel.

TABLE F-91 Configure Domains and Workgroups Panel

Field	Description
Domain	
Domain	The name of an existing domain. Domain names must not exceed the 15-character NetBIOS limit. **Note:** If you want to enable Active Directory Service (ADS), type the name of the Windows 2000 domain in which ADS is running. The system must also belong to this domain.

TABLE F-91 Configure Domains and Workgroups Panel *(Continued)*

Field	Description
User Name	The name of an existing domain user. User names can be up to 16 characters in length. If you want to enable ADS, the user name in this field must be for a Windows 2000 user with administrative rights. This user must be the domain administrator or a user that is a member of the domain Administrators group. The ADS client performs secure ADS updates with this user. **Note:** If the domain administrator user name is displayed in this field but the ADS update fails, the domain administrator password must be changed (on the domain controller). This is only required for the administrator user, and the same password can be reused. For more information, see the Microsoft Support Services Web Site, Article Q248808.
Password	The password of the domain user. For ADS, this is the Windows administrative user's password.
Enable ADS	Select if you want the Active Directory Service (ADS) software to publish Sun StorageTek shares to ADS or remove Sun StorageTek shares from ADS. For more information about ADS and how to configure it, see "About Active Directory Service" on page 76.
ADS Information	Information specific to the Active Directory Service: • Container - The ADS path location of the Windows 2000 administrative user in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation. **Note:** Do not include the domain name in the path. • Site - The local ADS NT domain name, assuming that a different subnet is used to control the ADS. This field must be blank if you do not have a local ADS site or if the same subnet is used by the domain specified on this panel and by the local ADS NT domain.
Kerberos Domain Information	Information specific to the Kerberos domain: • Realm - The Kerberos realm name that is used to identify ADS (this is usually the ADS domain). This is usually the ADS domain or the Domain Name Service (DNS) domain. When you click Apply, this entry is converted to all uppercase letters. • Server - The host name of the of the Kerberos Key Distribution Center (KDC) server. This is usually the host name of the primary domain controller in the ADS domain. If the software can locate the KDC server by using Domain Name Service (DNS) software, this field will be blank.
Workgroup	
Name	The name of the workgroup.
Comments	A line of text that describes the network configuration.

TABLE F-91 Configure Domains and Workgroups Panel *(Continued)*

Field	Description
Apply	Click to save your changes. If you are configuring Windows networking for a Windows NT domain, an account is automatically created on the domain for this system.
Cancel	Click to clear the fields of new entries and to return the values that were originally displayed on the panel.

Configure Groups Panel

This panel enables you to administer local groups. Privileges are granted to individual local groups rather than to individual users.

Note: Local groups apply only to environments that use Common Internet File System (CIFS) networking. For more information about local groups, see "About Local Groups" on page 84.

The following table describes the fields and elements on this panel.

TABLE F-92 Fields and Elements on the Configure Groups Panel

Field	Description
Groups	The groups of which the system is aware. When you choose a group from this menu, the Group Members and the Group Privileges menus are updated with information specific to that group.
Group Members	The users that are members of the selected group. For information about adding and removing users to and from a group, see "Adding and Removing Group Members and Configuring Privileges" on page 86.
Group Privileges	The privileges that are applied to the selected group. For more information about the supported group privileges, see "About Configuring Privileges for Local Groups" on page 84
Comment	A line of text that describes the group.
Apply	Click to save your changes.
Add Group	Click to launch the Add Group window. From this window, you can create a new group. For more information, see "Adding and Removing Group Members and Configuring Privileges" on page 86.

TABLE F-92 Fields and Elements on the Configure Groups Panel *(Continued)*

Field	Description
Edit Group	Click to launch the Edit Group window. From this window, you can edit the name and comment text for the selected group. You cannot edit the following default groups: Administrators, Backup Operators, and Power Users.
Remove Group	Click to delete the selected group. You cannot delete the following default groups: Administrators, Backup Operators, and Power Users.
Refresh	Click to update the panel with the latest information. **Note:** If you have made changes but you have not yet clicked Apply, clicking Refresh removes your changes from the panel.

Configure Mapping Policy Panel

If your system includes both UNIX and Windows environments, this panel enables you to establish rules for an equivalence relationship between UNIX users and groups and Windows users and groups.

Choosing a user and group mapping policy establishes credential equivalence on the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System to provide common access using either environment. For more information, see "About Mapping User and Group Credentials" on page 92.

The following table describes the fields and buttons on this panel.

TABLE F-93 Fields and Elements on the Configure Mapping Policy Panel

Field	Description
Windows <__> Unix User Mapping Choice	
Default Mapping	Select to establish no predefined mapping rule between Windows and UNIX users. New users are assigned newly-generated, unique user identifiers by the system.
Map by User Name	Select to map UNIX and Windows users who have identical user names. This enables the same user to access the Sun StorageTek 5320 NAS Appliance system, Sun StorageTek 5320 NAS Cluster Appliance, or Sun StorageTek 5320 NAS Gateway System from both environments.

TABLE F-93 Fields and Elements on the Configure Mapping Policy Panel *(Continued)*

Field	Description
Map by Full Name	Select to map UNIX and Windows users that have identical full names.
Windows <__> Unix Group Mapping Choice	
Default Mapping	Select to establish no predefined mapping rule between Windows and UNIX groups. New groups are assigned newly-generated, unique, group identifiers by the system
Map by Group Name	Select to map UNIX and Windows groups that have identical group names.
Map to Primary Group	Select to map to the NFS group in the primary group field in the configured `passwd` file. For more information, see "About Group Mapping" on page 96.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Maps Panel

This panel enables you to view existing mappings between UNIX users and groups and Windows users and groups. It also enables you to manually configure mappings between UNIX users and groups and Windows users and groups.

The following table describes the fields and buttons on this panel.

TABLE F-94 Fields and Elements on the Configure Maps Panel

Field	Description
Users	Select to display existing user mappings in the table.
Groups	Select to display existing group mappings in the table.
Unix Name	The name of the user or group as defined in the UNIX environment.
Unix ID	The unique identifier assigned to the user or group in the UNIX environment.
Windows Name	The name of the user or group as defined in the Windows environment.
Windows Domain	The domain to which the user or group belongs in the Windows environment.

TABLE F-94 Fields and Elements on the Configure Maps Panel *(Continued)*

Field	Description
Windows RID	The relative identifier (RID) assigned to the user or group in the Windows environment.
Add	Click to launch the Add SMB/CIFS User Map window or the Add SMB/CIFS Group Map window, depending on whether you selected Users or Groups at the top of the Configure Maps panel. From this window, you can configure a new user or group mapping. For more information, see "Mapping Windows Groups and Users to UNIX Groups and Users" on page 99.
Remove	Click to delete the selected user or group mapping, depending on whether you selected Users or Groups at the top of the Configure Maps Panel.
Edit	Click to launch the Edit SMB/CIFS User Map window or the Edit SMB/CIFS Group Map window, depending on whether you selected Users or Groups at the top of the Configure Maps panel. From this window, you can edit the selected user or group mapping. For more information, see "Editing a Mapping Between a Windows Group or User and a UNIX Group or User" on page 100.

Configure Shares Panel

This panel enables you to add, view, and update static Server Message Block (SMB) shares.

The table at the top of this panel shows information about all existing SMB shares on the system. This includes the share name and directories shared, as well as information that only concerns Windows Workgroups (user and group information, read/write password, and read-only password).

Note: After creating a volume, you must create a share for the volume. Users can then access the volume and create directories. After directories are created on the volume, you can create individual shares for them.

The following table describes the fields and buttons on this panel.

TABLE F-95 Fields and Buttons on the Configure Shares Panel

Field	Description
Name	The name of the share. This is the name that users see on the network. The name cannot be longer than 15 characters. The following characters are not supported: = | : ; \ " ? < > * /
Path	The location of the share on the system.
Comment	Information about the share.
User	The name of the user who owns the share.
Group	The group in which the user who owns the share belongs.
Umask	The file creation mask, if any, that is applied to this share. The umask defines the security policy for files and directories created in Share mode. It specifies the permission bits to turn off when a file is created. For more information, see "About Share Access Permissions" on page 105.
Container	This field is available only if you have enabled Active Directory Service (ADS) for the share on the "Configure Domains and Workgroups Panel" on page 397. The ADS container in which the share is published.
Desktop DB Calls	Whether the system can access and set Macintosh desktop database information. If the On value is displayed in this field, Macintosh client file access is sped up and non-Macintosh clients can access Macintosh files in this share.
Add	Click to create a new share. The Add Share window enables you to specify all share information.
Remove	Click to launch the Remove Share window. From this window, you can remove the share that you have selected in the table. You must click Yes to perform the actual removal.
Edit	Click to update information about the share that you have selected in the table.

Remove Share Window

This window enables you to remove a share from the configuration.

The following table describes the fields and buttons in this window.

TABLE F-96 Fields and Elements on the Remove Share Window

Field	Description
Name	The name of the share. This is the name that users see on the network. The name cannot be longer than 15 characters. The following characters are not supported: = | : ; \ " ? < > * /
User	The name of the user who owns the share.
Group	The group in which the user who owns the share belongs.
Apply	Click to remove the share from the configuration.
Cancel	Click to exit out of the window without saving any changes.

Set Up WINS Panel

If you are using a Windows or a mixed environment, this panel enables you to set up the Windows Internet Naming Service (WINS) server with the Sun StorageTek software.

The WINS server enables computers on your network to communicate with each other by resolving Network Basic Input/Output System (NetBIOS) names to Internet Protocol (IP) addresses. If Server Message Block (SMB) is enabled, your system has a NetBIOS name.

If you are using a pure UNIX environment, you do not need to set up WINS.

The following table describes the fields and buttons on this panel.

TABLE F-97 Fields and Buttons on the Set Up WINS Panel

Field	Description
Enable WINS	Select to enable WINS, which allows the system to be a WINS client.

TABLE F-97 Fields and Buttons on the Set Up WINS Panel *(Continued)*

Field	Description
Primary WINS Server	The IP address of the server that is consulted first for NetBIOS name resolution.
Secondary WINS Server	The IP address of the server that is consulted only if the primary WINS server is not responding.
Scope	The NetBIOS scope identifier, which must be a valid domain name as defined by the Domain Name Service (DNS) software. For more information about valid values that you can enter in this field, see "Setting Up WINS" on page 27.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

System Status Panel

This panel enables you to view general information about the network attached storage (NAS) system. In the bottom portion of the panel, the latest status of the system is displayed.

The following table describes the fields on this panel.

TABLE F-98 Fields on the System Status Panel

Field	Description
Name	The system name.
Model	The system model.
Serial #	The unique serial number of the system.
Up Time	The amount of time elapsed since the system was last turned on.
CPU Load	The current and peak central processing unit (CPU) load.
OS Version	The version of operating system currently running on the system.
Web Admin Version	The version designation for the graphical Web Administration application.

Index

B

C

D

E

F

G

M

N

O

P

Q

R

S

T

U

V

W