



# Sun StorEdge™ 5310 NAS Appliance Software Installation, Configuration, and User Guide

---

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 819-0879-12  
May 2005, Revision A

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

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, Sun StorEdge, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Mozilla is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries. Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

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

---

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuels relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuels peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, Sun StorEdge, Java, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Mozilla est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. Netscape et Netscape Navigator sont des marques de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



# Contents

---

- 1. Introduction 1**
  - About the Sun StorEdge 5310 NAS Appliance 1
  - About the Sun StorEdge 5310 Cluster 2
  - Other Sun StorEdge 5310 NAS Appliance Documentation 2
  - About This User's Guide 3
  - Software Requirements and Updates 4
  - Initial Sun StorEdge 5310 NAS Appliance Configuration 4
  - Navigating in Web Administrator 8
  - Running the Configuration Wizard 13
  - Where to Go from Here 15
  
- 2. Initial Network Configuration 17**
  - Setting the Server Name 18
  - Setting Logical Unit Number (LUN) Paths 19
  - Enabling Failover 24
  - Configuring the Network Ports 27
  - Setting the Default Gateway Address 30
  - Name Services 30
  - Setting Up Email Notification 41
  - Setting Up Logging 43

Assigning the Language	44
Where to Go from Here	45
<b>3. Initial File System Setup</b>	<b>47</b>
File System Concepts	47
Establishing a File System	50
Where to Go from Here	55
<b>4. System Management</b>	<b>57</b>
Setting the Administrator Password	57
Controlling the Time and Date	58
<b>5. Managing System Ports</b>	<b>63</b>
Sun StorEdge 5310 NAS Appliance Port Locations	63
About Alias IP Addresses	64
Configuring Network Ports	65
Port Bonding	65
<b>6. File System Management</b>	<b>73</b>
LUN Management	73
File Volume and Segment Management	74
<b>7. Name Services</b>	<b>79</b>
Active Directory Services	80
Setting Up LDAP	88
Setting Up WINS	89
Setting Up DNS	89
Setting Up NIS	89
Setting Up NIS+	89
Changing Name Service Lookup Order	89

<b>8. Group, Host, and File Directory Security</b>	<b>93</b>
Sun StorEdge 5310 NAS Appliance Local Groups	93
Configuring Hosts	99
Mapping User and Group Credentials	101
Setting File Directory Security	104
<b>9. Shares, Quotas, and Exports</b>	<b>109</b>
Shares	109
Managing Quotas	119
Setting Up NFS Exports	128
<b>10. Sun StorEdge 5310 NAS Appliance Options</b>	<b>133</b>
Activating Sun StorEdge 5310 NAS Appliance Options	133
Sun StorEdge File Replicator	136
Compliance Archiving Software	152
<b>11. Monitoring</b>	<b>155</b>
Monitoring Functions	155
Viewing Sun StorEdge 5310 NAS Appliance Status	157
System Logging	158
Environmental Status	161
Usage Information	165
Viewing Network Routes	169
Monitoring System Components	170
Viewing Backup Job Status	175
<b>12. System Maintenance</b>	<b>179</b>
Setting Remote Access Options	179
Configuring File Transfer Protocol (FTP) Access	181
Shutting Down the Server	183

Failover	184
Initiating Failback	186
File Checkpoints	188
Backup and Restore	199
Running a Head Cleaning	200
Updating Sun StorEdge 5310 NAS Appliance Software	201
<b>A. Console Administration</b>	<b>203</b>
Accessing The Console Administrator	203
Console Menu Basics	206
Viewing the Main Menu	206
Configuration Backup	208
System Management	208
Managing Routes	215
Name Services	218
Managing the Server File System	223
Shares and Quotas	230
Security	235
Mapping User and Group Credentials	238
Hosts	242
Monitoring	247
System Maintenance	254
<b>B. Sun StorEdge 5310 NAS Appliance Error Messages</b>	<b>263</b>
About SysMon Error Notification	263
Sun StorEdge 5310 NAS Appliance Error Messages	263
<b>C. Compliance Archiving Software API</b>	<b>269</b>
Compliance Features	270
Accessing Compliance Functionality	271

Behavior of UNIX System Calls	275
Behavior of Windows Clients	278
Other APIs	279
<b>D. Technical Support and Q&amp;A</b>	<b>281</b>
Sending a Diagnostic Email Message	281
Contacting Technical Support	282
<b>Glossary</b>	<b>285</b>
<b>Index</b>	<b>295</b>





# Figures

---

FIGURE 1-1	LCD Panel Without DHCP	6
FIGURE 1-2	Setting the Static IP Address	6
FIGURE 1-3	The Login Screen	7
FIGURE 1-4	The Main Window	9
FIGURE 1-5	The Toolbar	10
FIGURE 1-6	The Navigation Panel	11
FIGURE 1-7	The Content Panel Showing System Status	12
FIGURE 1-8	The System Events Panel	13
FIGURE 2-1	The Set Server Name Panel	18
FIGURE 2-2	LUN Paths Displayed on the Set LUN Path Panel	19
FIGURE 2-3	Single-Head System Configuration	20
FIGURE 2-4	Dual-Head System Configuration	21
FIGURE 2-5	The Set LUN Path Panel	22
FIGURE 2-6	Select Primary Path Dialog Box	23
FIGURE 2-7	The Enable Failover Panel	25
FIGURE 2-8	The Recover Panel	26
FIGURE 2-9	Configuring Network Adapters	28
FIGURE 2-10	The Set Gateway Address Panel	30
FIGURE 2-11	The Configure Domains and Workgroups Panel	31
FIGURE 2-12	The Set Up WINS Panel	33
FIGURE 2-13	The Set Up DNS Panel	35

FIGURE 2-14	The Set Up NIS Panel	37
FIGURE 2-15	The Set Up NIS+ Panel	39
FIGURE 2-16	The Configure Name Services Panel	40
FIGURE 2-17	The Set Up Email Notification Panel	42
FIGURE 2-18	The Set Up Remote Logging Panel	43
FIGURE 2-19	The Assign Language Panel	45
FIGURE 3-1	The Create File Volumes Panel	51
FIGURE 3-2	The Attach Segments Panel	54
FIGURE 3-3	Available Segments	55
FIGURE 4-1	The Admin Password Panel	57
FIGURE 4-2	The Set Up Time Synchronization Panel	59
FIGURE 4-3	The Set Time and Date Panel	61
FIGURE 5-1	The Bond NIC Ports Panel	67
FIGURE 5-2	The Create Port Bond Dialog Box	67
FIGURE 5-3	The Bond NIC Ports Panel	69
FIGURE 5-4	The Create Port Bond Dialog Box	69
FIGURE 5-5	Dual-Head Port Bonding	70
FIGURE 6-1	The Edit Properties Panel	74
FIGURE 6-2	The Delete File Volumes Panel	76
FIGURE 6-3	The View Volume Partitions Panel	77
FIGURE 7-1	The Set Time and Date Panel	81
FIGURE 7-2	The Configure Domains and Workgroups Panel	82
FIGURE 7-3	The Configure Name Services Panel	84
FIGURE 7-4	The Set Up DNS Panel	85
FIGURE 7-5	The Add Share Dialog Box	86
FIGURE 7-6	The Set Up NSSLDPAP Panel	88
FIGURE 7-7	The Configure Name Services Panel	90
FIGURE 8-1	The Configure Groups Panel	96
FIGURE 8-2	The Add Group Dialog Box	97
FIGURE 8-3	The Configure Groups Panel	98

FIGURE 8-4	The Set Up Hosts Panel	99
FIGURE 8-5	The Add Host Dialog Box	100
FIGURE 8-6	The Edit Host Dialog Box	100
FIGURE 8-7	The Configure Mapping Policy Panel	102
FIGURE 8-8	The Configure Maps Panel	103
FIGURE 8-9	The Add SMB/CIFS User Map Dialog Box	103
FIGURE 8-10	Mapping a Network Drive	105
FIGURE 8-11	The Map Network Drive Dialog Box	106
FIGURE 8-12	The Directory Permissions Dialog Box	107
FIGURE 9-1	The Configure Shares Panel	111
FIGURE 9-2	The Add Share Dialog Box	112
FIGURE 9-3	The Edit Share Dialog Box	115
FIGURE 9-4	The Configure Autohome Panel	118
FIGURE 9-5	The Configure User and Group Quotas Panel	120
FIGURE 9-6	The Add Quota Setting Dialog Box	121
FIGURE 9-7	The Configure User and Group Quotas Panel	122
FIGURE 9-8	The Edit Quota Setting Dialog Box	123
FIGURE 9-9	The Configure Directory Tree Quotas Panel	125
FIGURE 9-10	The Add DTQ Setting Dialog Box	126
FIGURE 9-11	The Edit DTQ Setting Dialog Box	127
FIGURE 9-12	The Configure Exports Panel	129
FIGURE 9-13	The Add NFS Export Dialog Box	130
FIGURE 9-14	The Edit NFS Export Dialog Box	131
FIGURE 10-1	The Activate Options Panel	134
FIGURE 10-2	The Set Time and Date Panel	135
FIGURE 10-3	The Secure Clock Initialization Dialog	135
FIGURE 10-4	The Mirror Relationship	136
FIGURE 10-5	The Configure Network Adapters Panel	138
FIGURE 10-6	The Add Mirror Dialog Box	140
FIGURE 10-7	The Manage Mirrors Panel	141

FIGURE 10-8	The Edit Mirror Dialog Box	142
FIGURE 10-9	The Set Threshold Alert Panel	143
FIGURE 10-10	The Manage Mirrors Panel	144
FIGURE 10-11	The Manage Mirrors Panel	145
FIGURE 10-12	The Promote Volume Dialog Box	146
FIGURE 10-13	The Mirror Relationship	147
FIGURE 10-14	The Delete File Volumes Panel	148
FIGURE 10-15	The Add Mirror Dialog Box	149
FIGURE 10-16	The Manage Mirrors Panel	151
FIGURE 10-17	The Change Volume Role Dialog Box	151
FIGURE 11-1	The Configure SNMP Panel	156
FIGURE 11-2	The System Status Panel	157
FIGURE 11-3	The Display System Log Panel	159
FIGURE 11-4	The View Fan Status Panel	161
FIGURE 11-5	The View Temperature Status Panel	162
FIGURE 11-6	The View Power Supply Status Panel	163
FIGURE 11-7	The View Voltage Regulator Status Panel	164
FIGURE 11-8	The View File Volume Usage Panel	166
FIGURE 11-9	The View Networking Activity Panel	166
FIGURE 11-10	The View System Activity Panel	167
FIGURE 11-11	Viewing Network Statistics	168
FIGURE 11-12	The View the Routing Table Panel	170
FIGURE 11-13	The Enabling UPS Monitoring Panel	172
FIGURE 11-14	The Mirror Statistics Panel	173
FIGURE 11-15	The View Backup Log Panel	175
FIGURE 11-16	The View Backup Status Panel	176
FIGURE 11-17	The View Tape Status Panel	177
FIGURE 12-1	The Set Remote Access Panel	180
FIGURE 12-2	The Set Up FTP Panel	182
FIGURE 12-3	The Shut Down the Server Panel	183

FIGURE 12-4	The Enable Failover Panel	186
FIGURE 12-5	The Recover Panel for Head Failback	187
FIGURE 12-6	The Recover Panel for Controller Failback	187
FIGURE 12-7	The Manage Checkpoints Panel	189
FIGURE 12-8	The Create Checkpoint Dialog Box	190
FIGURE 12-9	The Schedule Checkpoints Panel	191
FIGURE 12-10	The Add Checkpoint Schedule Dialog Box	192
FIGURE 12-11	The Edit Checkpoint Schedule Dialog Box	193
FIGURE 12-12	The Rename Checkpoint Dialog Box	194
FIGURE 12-13	The Configure Shares Panel	196
FIGURE 12-14	The Add Share Dialog Box	197
FIGURE 12-15	The Windows Start Menu	198
FIGURE 12-16	The Run Dialog Box	198
FIGURE 12-17	The Set Up NDMP Panel	199
FIGURE 12-18	The Assign Cleaning Slot Panel	200
FIGURE 12-19	The Update Software Panel	202
FIGURE A-1	The Telnet Screen	204
FIGURE A-2	The Connect Dialog Box	204
FIGURE A-3	The Telnet Connection Prompt	205
FIGURE A-4	The Main Menu	207
FIGURE A-5	The Extensions List	207
FIGURE A-6	Configuring the Host Name and Network Information	209
FIGURE A-7	The Admin Access Screen	210
FIGURE A-8	The Timezone, Time, Date Screen	211
FIGURE A-9	The NTP Configuration Screen	212
FIGURE A-10	The RDATE Time Update Screen	214
FIGURE A-11	The Language Selection Screen	215
FIGURE A-12	The Host Name and Network Screen	216
FIGURE A-13	The Manage Routes Screen	216
FIGURE A-14	The Edit Routes Screen	217

FIGURE A-15	The DNS and SYSLOGD Screen	218
FIGURE A-16	The Configure NIS and NIS+ Screen	221
FIGURE A-17	The Lookup Order Screen	222
FIGURE A-18	The Drive Letter Assignment Screen	223
FIGURE A-19	The Disks and Volumes Screen	224
FIGURE A-20	The Volume Creation Screen (1)	225
FIGURE A-21	The Volume Creation Screen (2)	225
FIGURE A-22	The Volume Creation Screen (3)	226
FIGURE A-23	The Configure Disk Screen	227
FIGURE A-24	The Segments Screen	228
FIGURE A-25	The Add an Extension Segment Screen (1)	228
FIGURE A-26	The Add an Extension Segment Screen (2)	229
FIGURE A-27	The SMB/CIFS Domain Configuration Screen	230
FIGURE A-28	The SMB/CIFS Autohome Setup Screen	231
FIGURE A-29	The SMB/CIFS Shares Screen	232
FIGURE A-30	The ADS Setup Screen	234
FIGURE A-31	The Local Groups Setup Screen	236
FIGURE A-32	The Modify Group Privileges Screen	238
FIGURE A-33	Users Map Setup Screen	239
FIGURE A-34	Users Map Setup Screen (2)	239
FIGURE A-35	The Group Map Setup Screen	241
FIGURE A-36	The New Host Screen	243
FIGURE A-37	The Trusted Hosts Screen	244
FIGURE A-38	The Trusted Host Access Screen	245
FIGURE A-39	The Volume Access Screen	246
FIGURE A-40	The SNMP Configuration Screen	248
FIGURE A-41	The Email Configuration Screen	249
FIGURE A-42	The Activity Monitor Screen	250
FIGURE A-43	The System Log Screen	251
FIGURE A-44	Viewing Port Bonding Information (page 1)	252

FIGURE A-45	Viewing Port Bonding Information (page 2)	252
FIGURE A-46	Checkpoint Analysis	253
FIGURE A-47	FTP Configuration	255
FIGURE A-48	The Shutdown Menu Screen	256
FIGURE A-49	The Failover/move LUNs Screen	257
FIGURE A-50	The LUN Ownership Screen	259
FIGURE A-51	The Configure LUN Path Screen	259
FIGURE A-52	The Configure Disk Screen	260
FIGURE A-53	The Checkpoint Configuration Screen	261
FIGURE D-1	The Diagnostic Email Dialog Box	282





# Tables

---

TABLE 1-1	Toolbar Icons	10
TABLE 2-1	LUN Paths in Single-Head Systems	20
TABLE 2-2	LUN Paths in Dual-Head Systems	21
TABLE 5-1	Dual-Head Port Bonding Example	71
TABLE 8-1	Sun StorEdge 5310 NAS Appliance Privileges	95
TABLE 8-2	Default Group Privileges	95
TABLE 9-1	Share Path Examples	110
TABLE 9-2	Umask Permission Examples	114
TABLE 11-1	System Event Icons	160
TABLE 11-2	Acceptable Voltage Ranges	165
TABLE A-1	Active Screen Keys	206
TABLE B-1	UPS Error Messages	264
TABLE B-2	File System Errors	266
TABLE B-3	RAID Error Messages	266
TABLE B-4	IPMI Error Messages	267
TABLE C-1	WORM File Metadata that Can and Cannot Be Modified	273



# Introduction

---

The Web Administrator graphical user interface (GUI) for the Sun StorEdge™ 5310 NAS Appliance makes it easy to set security and network configurations, and to perform administrative tasks on Sun Microsystems innovative Sun StorEdge 5310 NAS Appliance systems.

---

**Note** – The software features and functions described in this book apply to both the Sun StorEdge 5310 NAS Appliance system and the Sun StorEdge 5310 Cluster system.

---

---

## About the Sun StorEdge 5310 NAS Appliance

The Sun StorEdge 5310 NAS Appliance employs innovative hardware and software technology to bring you the industry's most efficient network attached storage.

The Sun StorEdge 5310 NAS Appliance supports file sharing between UNIX® and Windows environments, significantly accelerating file I/O services, and ensuring data integrity by relying on a fully journaling file system. It also optimizes application server performance by off-loading data sharing responsibilities.

The Sun StorEdge 5310 NAS Appliance attaches directly to the network as quickly and simply as a network printer, and features high-speed RAID controller architecture as well as redundant components that improve data availability. The modular, scalable Sun StorEdge 5310 NAS Appliance offers non-stop performance for users who require optimum file-sharing capabilities.

The Sun StorEdge 5310 NAS Appliance is designed for the workgroup or small business that needs to add a significant amount of additional storage, but cannot afford the time, manpower, or financial resources to managing a complex storage subsystem. It is a single-head system.

---

## About the Sun StorEdge 5310 Cluster

The Sun StorEdge 5310 Cluster with two Sun StorEdge 5300 RAID EU controller arrays provides high reliability and high availability network attached storage (NAS) services, using an active/active pair of servers in a system configuration with no single point of failure.

The servers in a Sun StorEdge 5310 Cluster system are similar to those used in stand-alone Sun StorEdge 5310 NAS Appliance configurations, with two key exceptions:

- High Availability (HA) servers are sold as matched pairs, identified as “-H1” and “-H2” in their software serial numbers, representing the head number
- Servers include support for peer health monitoring

Storage in a Sun StorEdge 5310 Cluster system is based on the same Sun StorEdge 5300 RAID EU controller arrays used in Sun StorEdge 5310 NAS Appliance systems, configured to support independent storage access from either or both servers, and optionally including Sun StorEdge 5300 EU expansion enclosures.

---

## Other Sun StorEdge 5310 NAS Appliance Documentation

The Sun StorEdge 5310 NAS Appliance package includes a printed *Setup Poster* which quickly guides you through hardware and software setup.

The Sun StorEdge 5310 Cluster package includes a printed *Sun StorEdge 5310 Cluster Setup Instructions*.

---

**Note** – The *Setup Poster* pertains to the non-clustered Sun StorEdge 5310 NAS Appliance and is not intended for setting up the Sun StorEdge 5310 Cluster system.

---

Documentation is available on the Sun web site at  
[http://www.sun.com/hwdocs/Network\\_Storage\\_Solutions/nas](http://www.sun.com/hwdocs/Network_Storage_Solutions/nas)

Refer to the *Sun StorEdge 5310 Release Notes* on the web site for last minute updates and changes.

Other online documentation includes:

- The *Sun StorEdge 5310 NAS Appliance Quick Reference Manual* which provides a shorter version of the hardware setup and software instructions contained in this software guide.
- The *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide* which provides detailed information and procedures for installing, connecting, and using the hardware components of the Sun StorEdge 5310 NAS Appliance system.

---

## About This User's Guide

This guide is designed as a user reference and operational guide to the Web Administrator GUI interface for the Sun StorEdge 5310 NAS Appliance and the Sun StorEdge 5310 Cluster.

The procedures and screen shots in this guide are intended to help you perform system tasks. Because the information displayed by the Web Administrator software is based on your Sun StorEdge 5310 NAS Appliance configuration, the actual screens displayed on your monitor may not be the same as the screen shots shown in this guide.

## Conventions Used in This Guide

This guide was designed to make it easy for you to find the information you need quickly. Familiarize yourself with the following:

Convention	Meaning
<i>Italic</i>	Points out cross references to other sections in this guide, identifies the titles of other documents, and emphasizes key terms and definitions.
<b>Bold</b>	Identifies keystrokes, menu items, window components (for example, panel titles or field labels), and mouse commands.
C:	Disk drives, such as drive A, drive C, or network drives, are referred to as A:, C:, etc.
Click	Press and release the left mouse button.
admin	Words in <i>Courier</i> type indicate typed commands or prompts.

---

# Software Requirements and Updates

The Sun StorEdge 5310 NAS Appliance ships with the Web Administrator software installed. Other than a standard Web browser, you do not need to install any software to manage your Sun StorEdge 5310 NAS Appliance system.

## Web Administrator Requirements

To access the Web Administrator management interface, you must have the following software:

- Windows 98/NT/2000/XP, Sun Solaris™ Operating System 5.7 (or later), or Red Hat Linux
- Internet Explorer 5.5 (or later) on systems using Windows 98/NT/2000/XP

or

- Netscape™ software 4.77 (or later) on systems using Windows 98/NT/2000/XP and Sun Solaris OS. **Netscape 6.0 and 6.01 are not supported.**
- Mozilla™ browser
- Java™ platform-enabled browser with Java Plug-In 1.3.1 (or later).

---

**Note** – To download the latest Java Plug-In, go to <http://java.com>.

---

---

## Initial Sun StorEdge 5310 NAS Appliance Configuration



---

**Caution** – These instructions are for the Sun StorEdge 5310 NAS Appliance only. For cluster configuration instructions, refer to the *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide* or the printed *Sun StorEdge 5310 Cluster Setup Instructions*.

---

To complete the initial Sun StorEdge 5310 NAS Appliance configuration, you must:

- Provide an IP address
- Access the Wizard through the Web Administrator
- Follow the instructions provided by the Wizard

# IP Address Configuration

To configure the Sun StorEdge 5310 NAS Appliance system, you must have an IP address for the system. You can assign an IP address in one of two ways:

- Automatic IP address assignment through a Dynamic Host Configuration Protocol (DHCP) server
- Manual IP address assignment through the Liquid Crystal Display (LCD) panel on the Sun StorEdge 5310 NAS Appliance

## Automatic (DHCP) IP Address Configuration

To dynamically acquire an IP address through a DHCP server, you must either have an existing DHCP server on the network or have a DHCP relay agent on the network with an accessible DHCP server on another network. (If a DHCP server is not available, you must input the IP address through the LCD panel on the front panel of the Sun StorEdge 5310 NAS Appliance.)

---

**Note** – If your system uses DHCP to assign Domain name System (DNS) and Windows Internet Naming Service (WINS) as well as IP and gateway addresses, the corresponding fields in the Wizard and Web Administrator screens are dynamically configured. Verify the information when it is presented by the Wizard during system configuration.

---

If your system supports DHCP, the DHCP server automatically assigns an IP address when the Sun StorEdge 5310 NAS Appliance boots up for the first time.

---

**Note** – To avoid waiting for DHCP discovery during the boot sequence, you can press any key on the LCD panel and confirm the “Abort DHCP?” message by pressing the Right-arrow key on the panel. Then you can manually set the static IP address following the instructions below.

---

## Manual IP Address Configuration

If a DHCP server is not available, you must configure the IP address using the LCD panel.

To configure the IP address using the LCD panel:

1. Turn on the Sun StorEdge 5310 NAS Appliance and wait for the boot sequence to complete. The LCD panel displays the following:



FIGURE 1-1 LCD Panel Without DHCP

---

**Note** – To avoid waiting for DHCP discovery during the boot sequence, you can press any key on the LCD panel and confirm the “Abort DHCP?” message by pressing the Right-arrow key on the panel.

---

2. Press the Select button once, then select Set Static IP.



FIGURE 1-2 Setting the Static IP Address

3. Enter or accept the values listed below, then move the cursor to the far right to save them:
  - IP address
  - Subnet mask
  - Broadcast address
  - Gateway address (if necessary)

To enter data, use the Up- and Down-arrows to select digits, dots, or spaces. Then use the Right-arrow to accept each character.

## Accessing the Web Administrator

---

**Note** – Before you can access Web Administrator, you must have connected the Sun StorEdge 5310 NAS Appliance to your network, provided an IP address, and prepared a client browser on the same network as the Sun StorEdge 5310 NAS Appliance.

---



## Connecting to the Web Administrator

When you connect to the Web Administrator for the first time, the Configuration Wizard launches automatically. If you need instructions for navigating within the Web Administrator, see "Navigating in Web Administrator" on page 8. Otherwise, proceed to "Running the Configuration Wizard" on page 13.

To connect to the Web Administrator:

1. **From a client on the same network, open a web browser and type the IP address of the Sun StorEdge 5310 NAS Appliance in the address or location field, for example:**

**http://123.111.78.99**

and press **Enter**.

---

**Note** – If you are using a proxy server and have trouble connecting, try enabling the browser option to bypass the proxy server for local addresses. See your browser's online help or documentation for more information.

---

The Web Administrator GUI interface for the Sun StorEdge 5310 NAS Appliance appears in your browser with a login screen.



**FIGURE 1-3** The Login Screen

---

**Note** – Once you reach the login screen, you may want to bookmark it or add it to your favorites so that you do not have to remember the IP address in the future.

---

2. **By default a password is not specified. Simply click the Apply button to access the system. For information on changing the administrator password, refer to "Setting the Administrator Password" on page 57.**

The End User License Agreement screen appears.


3. **Accept or decline the license agreement. If you decline, Web Administrator returns you to the main login screen. If you accept, the Configuration Wizard starts automatically.**
4. **Follow the on-screen prompts, entering information as requested. For more detailed descriptions of the Wizard screens, see "Starting the Wizard" on page 14. If your system uses DHCP to assign DNS, WINS, or IP and gateway addresses, these fields are automatically configured. When you reach these screens in the Wizard, verify the information, then continue with the Wizard.**

---

## Navigating in Web Administrator

The Web Administrator GUI interface for the Sun StorEdge 5310 NAS Appliance is an easy-to-use graphical user interface that lets you configure system parameters through a series of menus and tab screens, or panels. These tab screens and settings are discussed in later chapters. If at any point you want to return to the main screen,

click  (Home button) from the toolbar.

If you need help in any screen, click  (Help button).

## Logging In

For all users, the normal login procedure is:

1. **Access the Login screen as described in "Connecting to the Web Administrator" on page 7.**

The **User Name**, *Admin*, is permanent and unchangeable.

2. Enter the Password in the field provided.

By default, a password is not specified. For information about setting the administrator password, refer to "Setting the Administrator Password" on page 57.

3. Click the Cancel button to exit the login screen or click the Apply button to login.

## Using the Graphical User Interface

The main window of Web Administrator lets you navigate, configure, and view Sun StorEdge 5310 NAS Appliance system events and services. The appearance of this window varies based on your hardware configuration.

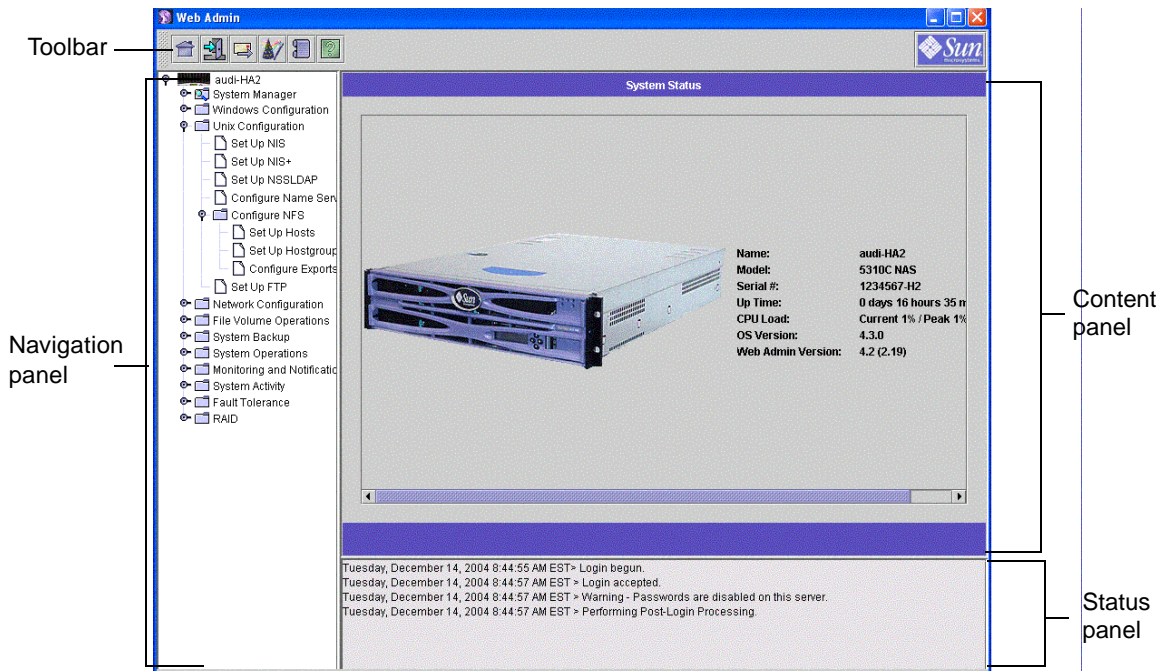


FIGURE 1-4 The Main Window

## The Toolbar







The toolbar at the top of the Web Administrator window lets you access the home status screen, log out, send a diagnostic email, run the configuration Wizard, access the system log, and access help pages.



**FIGURE 1-5** The Toolbar

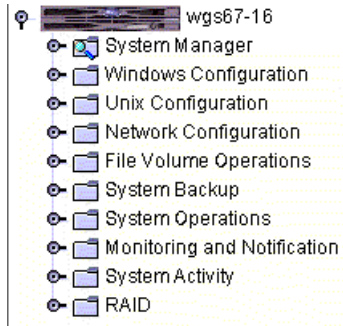
The toolbar icons run the following tasks:

**TABLE 1-1** Toolbar Icons




	View the home system status screen
	Log out
	Send a diagnostic email
	Run the configuration Wizard
	Access the system log
	Access help

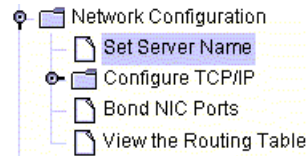
## The Navigation Panel



Use this panel to navigate within the Web Administrator. You can access all configuration, setup, and administrative functions through the navigation panel.



**FIGURE 1-6** The Navigation Panel

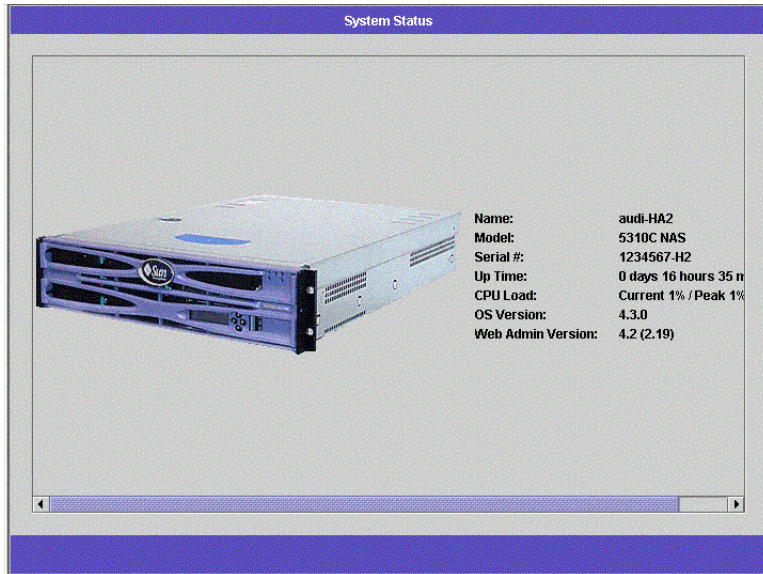
To open a folder, click the  symbol next to the folder. It changes to the  position. For example:  Network Configuration becomes:



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

## Content Panel

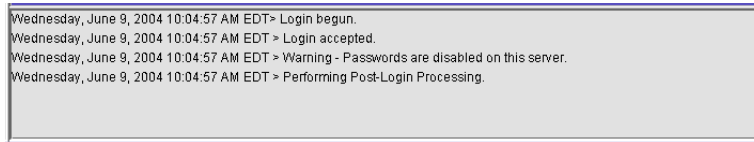
This panel contains the Sun StorEdge 5310 NAS Appliance general system information.



**FIGURE 1-7** The Content Panel Showing System Status

## System Events Panel


At the bottom of the Web Administrator window, the system events panel displays all events that have occurred since the last login. 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.



**FIGURE 1-8** The System Events Panel

## Using Help

Help screens are available in every tab screen of the Web Administrator to provide more detailed information regarding the terms, fields, checkboxes, option buttons (radio buttons), and action buttons in that screen.

To reach the help screen for any Web Administrator topic, click the  button, located in the toolbar. The corresponding help window for the content panel currently displayed appears alongside the Web Administrator screen.

---

## Running the Configuration Wizard

The configuration wizard runs automatically the first time you log on. The wizard is designed to guide you through the initial setup of your Sun StorEdge 5310 NAS Appliance. It helps you complete all of the steps necessary to establish communication between the Sun StorEdge 5310 NAS Appliance and your network. Once you complete the wizard, you still need to set up your file system and configure user access.

## Configuration Wizard Variations

The configuration wizard offers several options. Some of these options are automatically determined by the Sun StorEdge 5310 NAS Appliance itself. Other options are determined by you, based on the network environment you are running.

This guide cannot cover all of the possible 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 Sun StorEdge 5310 NAS Appliance. 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 wizard's path. These three paths are:

- **UNIX Only**—This path helps you configure the Sun StorEdge 5310 NAS Appliance for operation in a pure UNIX network. It skips over all Windows-dependent features and functions.
- **Windows Only**—This path helps you configure the Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance for a mixed network environment combining Windows and UNIX features.

Select the path appropriate to your network environment.

## Starting the Wizard



To run the configuration wizard, click the  icon on the tool bar. The wizard opens to an introductory page. Click **Next** to proceed. The wizard then progresses through the following steps, which are described in more detail in Chapter 2, "Initial Network Configuration":

1. **Setting the server name and contact information**
2. **Configuring network adapters**
3. **Setting the default gateway**
4. **Configuring Domains and Workgroups (Windows environments and mixed environments) and enabling and configuring Active Directory Service (ADS) (Windows environments and mixed environments)**
5. **Configuring WINS (Windows environments and mixed environments)**



## 6. Setting up DNS

---

**Note** – If the system started up using DHCP, confirm that the address of the DNS server is correct. If not, uncheck the “Configure DNS” checkbox to avoid delays in restarts and failovers.

---

7. **Setting up Network Information Service (NIS) (UNIX environments and mixed environments)**
8. **Setting up Network Information Service Plus (NIS+) (UNIX environments and mixed environments)**
9. **Configuring name services (UNIX environments and mixed environments)**
10. **Setting up email notification**
11. **Setting up remote and local logging**
12. **Assigning the language**
13. **Confirming your settings**

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

If you do not want to run the wizard, Chapter 2, “Initial Network Configuration” describes accessing the same functions in the same sequence through the navigation panel.

---

## Where to Go from Here

At this point, the Sun StorEdge 5310 NAS Appliance should be up and running and you should have a basic understanding of how to get around in Web Administrator. From here you need to establish your file system and configure user access.

Setting up your file system includes any LUNs, Partitions, File Volumes, and Segments that you need to establish. See “File System Concepts” on page 47 for more information on these concepts.

When your file system is complete, you must set up user access rights and any other system management features. Chapter 4, “System Management” on page 57, covers the basic management functions. Refer to 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.



## Initial Network Configuration

---

This chapter describes configuring your Sun StorEdge 5310 NAS Appliance for communication on your network. After you configure network communication and services, you still 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. It does not cover all of the features you may 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.



---

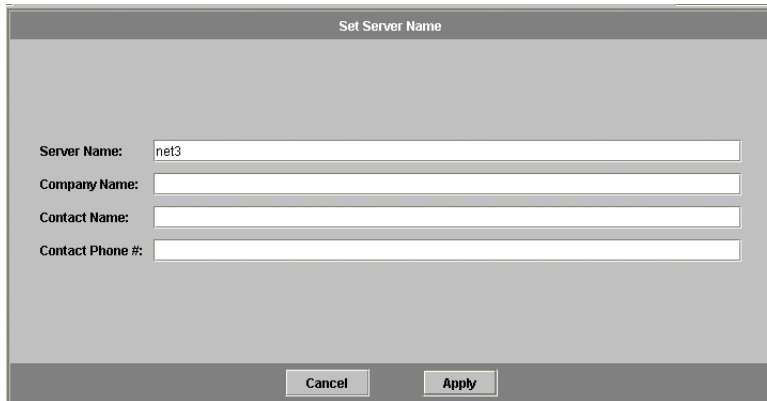
**Caution** – After you have completed system configuration, you should back up the configuration information in the event of a system failure. Refer to "Configuration Backup" on page 208 for details on backing up configuration information.

---

# Setting the Server Name

To set the Sun StorEdge 5310 NAS Appliance server name as it will appear on the network:

1. In the navigation panel, select **Network Configuration > Set Server Name**.



**FIGURE 2-1** The Set Server Name Panel

2. Enter the Sun StorEdge 5310 NAS Appliance server name in the Server Name box. This name identifies the Sun StorEdge 5310 NAS Appliance (or this head unit, for Sun StorEdge 5310 Cluster systems) on the network. The server name can include alphanumeric (a-z, A-Z, 0-9), "-" (dash), "\_" (underscore), and "." (period) characters.

---

**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. Enter the contact information for your company, including your company name and contact information for the Sun StorEdge 5310 NAS Appliance administrator. The Sun StorEdge 5310 NAS Appliance includes this information in any diagnostic email messages sent. For more information about diagnostic email messages, refer to "Sending a Diagnostic Email Message" on page 281.
4. Click **Apply** to save your settings.

---

# Setting Logical Unit Number (LUN) Paths

## About LUN Paths

A LUN path is a designation that describes how a file volume in a LUN is accessed by what head and controller. To every file volume there are two LUN paths: 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 StorEdge 5310 Cluster system, a head induces a head failover (see "About Head Failover" on page 24) should the alternate path fail.

LUN paths can be viewed and edited (see "Setting LUN Paths" on page 22) on the Set LUN Path panel.

LUN	Volumes	Active Path	Primary Path	Alternate Path
ffk1d010	/vol1 /vol1 /tpvol /test 460.1GB	1/1	1/1	1/0
ffk1d001	/postvol ~a 550.4GB	1/0	1/0	1/1

**FIGURE 2-2** LUN Paths Displayed on the Set LUN Path Panel

- LUN — This column lists the available LUNs on the system.
- Volumes — This column lists the file volume names. There may be more than one file volume in a LUN.
- Active Path — This column lists the currently active LUN path.

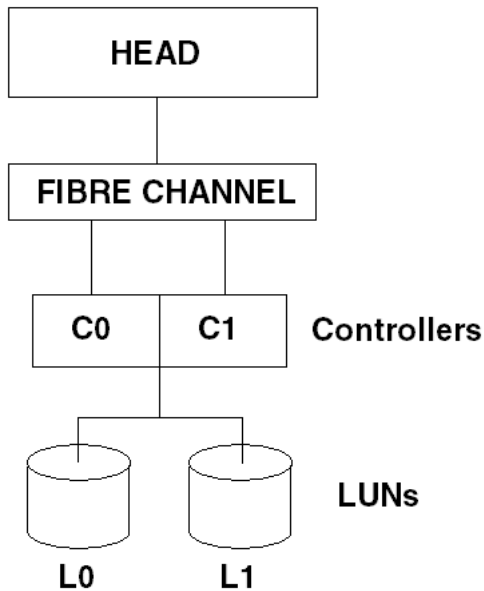
"1/1" designates controller 1 and its active state. The first number designates the HBA number. A system can have multiple HBAs starting from 1. The second number designates the SCSI (target) of the controller.

For example, "1/0" designates HBA 1 and SCSI controller target 0.

- **Primary Path** — This column lists the primary LUN paths, the paths the system selects during system initiation. They are also the paths to which a LUN path can be “restored.” If a primary path is not specified, the system will use the first available path.
- **Alternate Path** — This column lists the paths that are used when the primary paths fails.

## LUN Paths in Single-Head Systems

The following illustrates a typical hardware configuration in a single-head system:



**FIGURE 2-3** Single-Head System Configuration

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

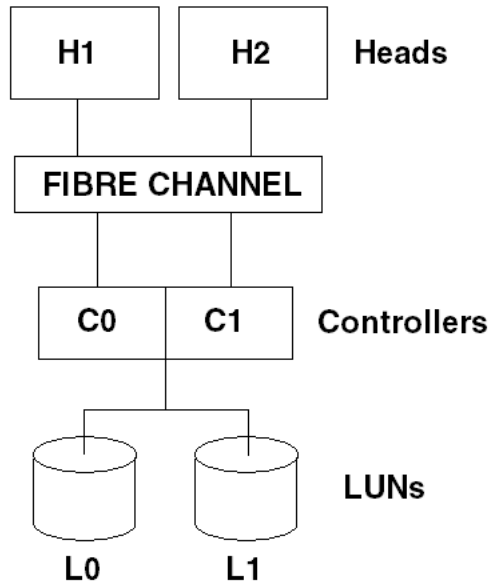
**TABLE 2-1** LUN Paths in Single-Head Systems

<b>Paths</b>	<b>LUN0</b>	<b>LUN1</b>
<b>Primary</b>	C0-L0	C1-L1
<b>Alternate</b>	C1-L0	C0-L1

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

## LUN Paths in Dual-Head Systems

The following illustrates a typical hardware configuration in a Sun StorEdge 5310 Cluster system:



**FIGURE 2-4** Dual-Head System Configuration

The primary LUN path on Head 1 is C0-L0; the alternate path is C0-L1. The primary LUN path on Head 2 is C1-L0 and the alternate path is C1-L1. As illustrated, the system would have the following LUN paths:

**TABLE 2-2** LUN Paths in Dual-Head Systems

Head 1	LUNs	LUN0	LUN1
	Paths	C0-L0	C0-L1
Head 2	LUNs	LUN0	LUN1
	Paths	C1-L0	C1-L1

File volumes are normally accessed through the primary LUN path designated for the LUN to which the file volumes belong. In a dual-head configuration, a head induces a failover should its primary and alternate paths fail (see "About Head Failover" on page 24).

# Setting LUN Paths

By setting a 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, the active path should be set to the primary path. A LUN can be reassigned only if there are no filesystems on that LUN. On a Sun StorEdge 5310 Cluster system, only the head that “owns” a LUN can reassign it to another head.

---

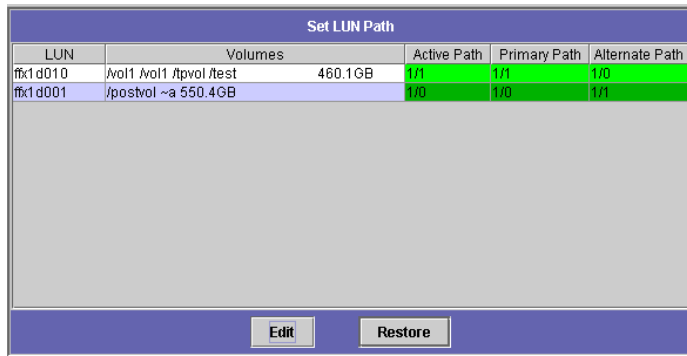
**Note** – On a Sun StorEdge 5310 Cluster system, when you first start the system, all LUNs are assigned to one head (Head 1). You must use Head 1 to reassign some LUNs to Head 2 for even distribution.

---

The Set LUN Path panel allows you to set active paths. In a Sun StorEdge 5310 Cluster system you can set an unassigned path from any head.

To set a LUN path:

1. In the navigation panel, select **Fault Tolerance > Set LUN Path**.



LUN	Volumes	Active Path	Primary Path	Alternate Path
ffx1d010	/vol1 /vol1 /tpvol /test 460.1GB	1/1	1/1	1/0
ffx1d001	/postvol ~a 550.4GB	1/0	1/0	1/1

**FIGURE 2-5** The Set LUN Path Panel

---

**Note** – LUNs that have no LUN path assigned may 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 shown once, on its current path.

---



2. Select a LUN and click Edit.

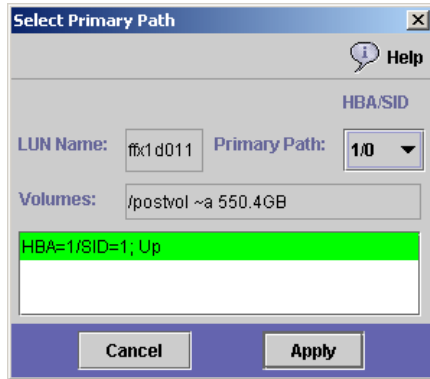


FIGURE 2-6 Select Primary Path Dialog Box

3. Select the desired controller from the Primary Path drop-down list.

Example: The drop-down option “1/0” assigns the selected LUN to controller 0 (C0). Option value “X/Y”: The “X” value is either 0 or 1. 1 designates that the controller is active; 0, inactive.

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

4. Click Apply.

## Restoring a LUN Path

A LUN’s current active path can be different from the its primary path. The “Restore” option on the Set LUN Panel allows you to restore a LUN’s current active path to its primary LUN path.

---

**Note** – Restoring a LUN path does not recover any data; it is not a disaster recovery function.

---

To restore a LUN path:

1. In the navigation panel, select **Fault Tolerance > Set LUN Path**.
2. Select the LUN and click **Restore**.

---

# Enabling Failover

Enabling failover is only valid for Sun StorEdge 5310 Cluster systems.

## About Head Failover

A Sun StorEdge 5310 Cluster system consists of a pair of active-active servers, called *heads*, that share access to the RAID controllers and several different networks. The RAID controllers are connected to each head through fibre controllers. A dedicated heartbeat cable connects the first NIC of the two heads and lets each head monitor the other head's health status.

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

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 **Fault Tolerance > Recover**, determine which LUNs are managed by which head.

## Enabling Head Failover

In the event of a head failure, failover causes the working head to take temporary ownership of the IP addresses and LUNs formerly managed by the failed head.

---

**Note** – When you enable head failover, DHCP is automatically disabled.

---

To enable head failover:

1. In the navigation panel, select **Fault Tolerance > Enable Failover**.

The screenshot shows the 'Enable Failover' configuration window. At the top, the title is 'Enable Failover'. Below the title, there is a checked checkbox labeled 'Automatic Failover'. Underneath, the 'Head Status' is displayed as 'NORMAL'. A section titled 'Link Failover' contains an unchecked checkbox for 'Enable Link Failover'. Below this, there are two input fields: 'Down Timeout' with the value '60' and 'Restore Timeout' with the value '60'. A section titled 'Partner Configuration' contains three input fields: 'Name' with the value 'p2', 'Gateway' with three asterisks, and 'Private IP' with the value '10 + 10 + 10 + 2'. At the bottom of the window are two buttons: 'Cancel' and 'Apply'.

**FIGURE 2-7** The Enable Failover Panel

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 which 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.

4. Then 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

You must manually initiate recovery (failback) of your Sun StorEdge 5310 NAS Appliance or Sun StorEdge 5310 Cluster system after it has undergone head or controller failover.

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

For example volume A was assigned to Head1 which had failed, so Head2 took ownership of volume A during the failover. Now that Head1 is fully functional again, it can recover its ownership of volume A from Head2.



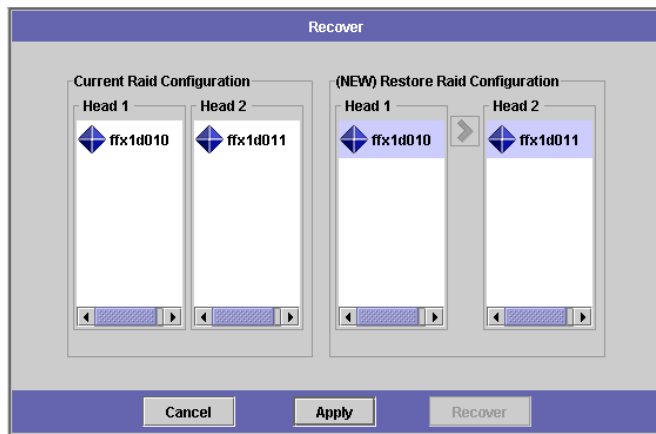
---

**Caution** – Make sure that the failed head is fully operable before attempting recovery.

---

To initiate recovery:

1. In the navigation panel, select **Fault Tolerance > Recover** to access the Recover panel.



**FIGURE 2-8** The Recover Panel

2. Select (highlight) the RAID set to be recovered.
3. Click Recover.

---

# Configuring the Network Ports

You can either enable DHCP or specify the 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 StorEdge 5310 Cluster 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 "Port Bonding" on page 65.

## Sun StorEdge 5310 NAS Appliance Port Locations

The Sun StorEdge 5310 NAS Appliance identifies ports in a predefined order based on their type and their physical and logical location on the server. Refer to your *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide* to identify the network port locations for configuration. Note that system configurations vary and those shown are examples.

The relationship of network interface cards (NICs) to ports is shown in the *Hardware User Guide*.

## Configuring Network Adapters

To configure network adapters:

1. In the navigation panel, select Network Configuration > Configure TCP/IP > Configure Network Adapters.



FIGURE 2-9 Configuring Network Adapters

2. If your network uses a DHCP server to assign IP addresses and you want to enable it, select the Enable DHCP checkbox.

Enabling DHCP allows the Sun StorEdge 5310 NAS Appliance server 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 "Port Bonding" on page 65 for more information on creating and setting up aggregate ports.

---

**Note** – On Sun StorEdge 5310 Cluster 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 "Port Bonding" on page 65 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. **For each port, select one of the following roles (for more details about port roles, refer to "Sun StorEdge 5310 NAS Appliance Port Locations" on page 63):**

- **Primary**—The port role of **Primary** identifies an active network port.

---


**Note** – At least one port 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.
- **Mirror**—The port role of **Mirror** shows that the port connects this server to another server to mirror file volumes.
- **Private**—**Sun StorEdge 5310 Cluster 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.

7. **To add an alias IP address to the selected port, enter it in the IP-Aliases field.**

Then click  to add it to the IP-Aliases list.

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

8. **Repeat for all ports in the Adapter list.**

9. **Click Apply to save your changes.**

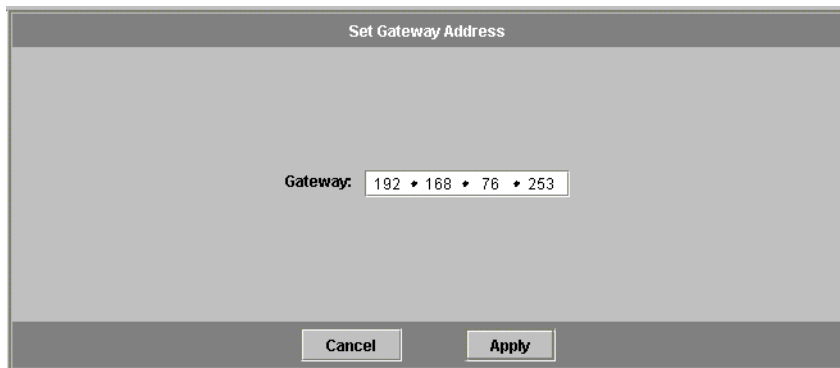
---

# Setting the Default Gateway Address

The default gateway address is the 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.

To specify the default gateway address for the Sun StorEdge 5310 NAS Appliance server:

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



**FIGURE 2-10** The Set Gateway Address Panel

2. Enter the gateway address in the Gateway text box.
3. Click **Apply** to save your settings.

---

# Name Services

This section describes setting up Windows security, WINS, DNS, NIS, NIS+, and configuring name services.

For more detail about name services, refer to Chapter 7, "Name Services" on page 79.



# Configuring 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.

Enable Windows Workgroup, NT Domain security, or ADS through the **Configure Domains and Workgroups** panel. By default, your Sun StorEdge 5310 NAS Appliance is configured in Windows Workgroup mode, with a workgroup name of “workgroup.”

To configure Windows security:

1. In the navigation panel, select **Windows Configuration > Configure Domains and Workgroups**.

The screenshot shows a window titled "Configure Domains and Workgroups". It has two radio buttons: "Domain" (selected) and "Workgroup". Under "Domain", there are three input fields: "Domain:" with "WG4DOMAIN", "User Name:" with "admin", and "Password:" with "\*\*\*\*\*". To the right, there is a checked checkbox "Enable ADS" and an "ADS Information" section with "Container:" set to "test" and "Site:" empty. Below that is a "Kerberos Domain Information" section with "Realm:" and "Server:" both empty. Under "Workgroup", there is a "Name:" field (empty) and a "Comments:" field with "Sun StorEdge 5210". At the bottom are "Cancel" and "Apply" buttons.

**FIGURE 2-11** The Configure Domains and Workgroups Panel

2. To enable Windows domain security, select the **Domain** option button. 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.

Then enter the following:

- a. Enter the name of the domain in the **Domain** field. This name must conform to the 15-character NetBIOS limitation.

- b. Enter the name and password of the administrative domain user in the User Name and Password fields. The user name can be 16 characters or fewer.
3. To enable Windows workgroup security, click the Workgroup option button. Then enter the name of the workgroup in the Name field. This name must conform to the 15-character NetBIOS limitation.
4. In the Comments field, enter a description of the Sun StorEdge 5310 NAS Appliance server (optional).
5. To enable ADS, click the Enable ADS checkbox. For more detail about ADS, refer to "Active Directory Services" on page 80.

---

**Note** – Prior to enabling ADS, you must verify that the Sun StorEdge 5310 NAS Appliance time is within five minutes of any ADS Windows 2000 domain controller. To verify the Sun StorEdge 5310 NAS Appliance time, select **System Operations > Set Time and Date** from the navigation panel.

---

Then enter the following:

- a. In the Domain field, enter the Windows 2000 Domain in which ADS is running. The Sun StorEdge 5310 NAS Appliance must belong to this domain.
- b. In the User Name field, enter the user name of a Windows 2000 user account with administrative rights. This person 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, you must change the domain administrator password (on the domain controller). Only the administrator user must do this and can reuse the same password. For more information, refer to the Microsoft Support Services Web site, Article Q248808.

---

- c. In the Password field, enter the Windows 2000 administrative user's password.
- d. 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. For more information, see "Active Directory Services" on page 80.

---

**Note** – Do not include the domain name in the path.

---

- e. Enter the name of the local ADS site in the Site field if it differs from the ADS Domain. Otherwise, leave the field blank.

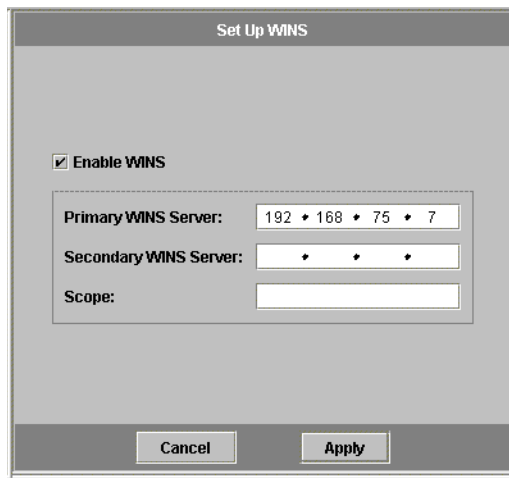
- f. In the Kerberos Realm Info section, enter the Realm name used to identify ADS. This is normally the ADS domain or the DNS domain. When you click Apply, this entry is converted to all upper-case letters.
  - g. In the Server field, enter the host name of the Kerberos Key Distribution Center (KDC) server. This is usually the host name of the primary domain controller in the ADS domain. You can leave this field blank if the Sun StorEdge 5310 NAS Appliance can locate the KDC server through DNS.
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 Name Services (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**.



**FIGURE 2-12** The Set Up WINS Panel

2. To enable WINS, click the Enable WINS checkbox. Checking this box makes the Sun StorEdge 5310 NAS Appliance server a WINS client.
3. Enter the 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 Sun StorEdge 5310 NAS Appliance consults the secondary WINS server.

**5. Enter the NetBIOS Scope identifier (optional) in the Scope field.**

Defining a scope will prevent this computer from communicating with any systems that do not have the same scope configured. Caution should therefore 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

DNS (Domain Name System) resolves host names to IP addresses for your Sun StorEdge 5310 NAS Appliance system.

---

**Note** – If you are using DNS without Dynamic DNS, add the Sun StorEdge 5310 NAS Appliance server's host name and IP address 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.

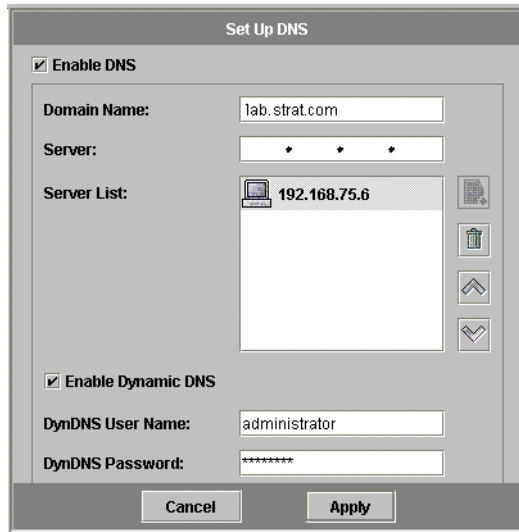






FIGURE 2-13 The Set Up DNS Panel

2. Select the Enable DNS checkbox.
3. Enter the DNS server Domain Name.
4. Enter the IP address of a DNS Server you want to make available to the network, then click the  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 Sun StorEdge 5310 NAS Appliance 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  or  buttons. To remove a server from the list, select the server IP address and click .
6. Select the Enable Dynamic DNS checkbox to let a Dynamic DNS client add the Sun StorEdge 5310 NAS Appliance 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 31. If you enable Dynamic DNS by selecting this checkbox, non-secure dynamic updates occur automatically if they are allowed by the DNS server.

7. To enable secure Dynamic DNS updates, complete the following information. This information is not required for non-secure updates.
  - a. In the DynDNS User Name field, enter the user name of a Windows 2000 user authorized to perform Dynamic DNS updates. This user account must reside within the ADS domain and Kerberos realm specified in the Configure Domains and Workgroups panel described in "Configuring Windows Security" on page 31.

---

**Note** – If you enter the domain administrator name here and the ADS update fails, the domain administrator must change the password (on the domain controller). Only the administrator user must do this, and the same password can be reused. For more information, refer to the Microsoft Support Services Web site, Article Q248808.

---

- b. In the DynDNS Password, enter the password of the DynDNS user. If you update this field, delete the entire password before entering a new one.
8. Click Apply to save your settings.

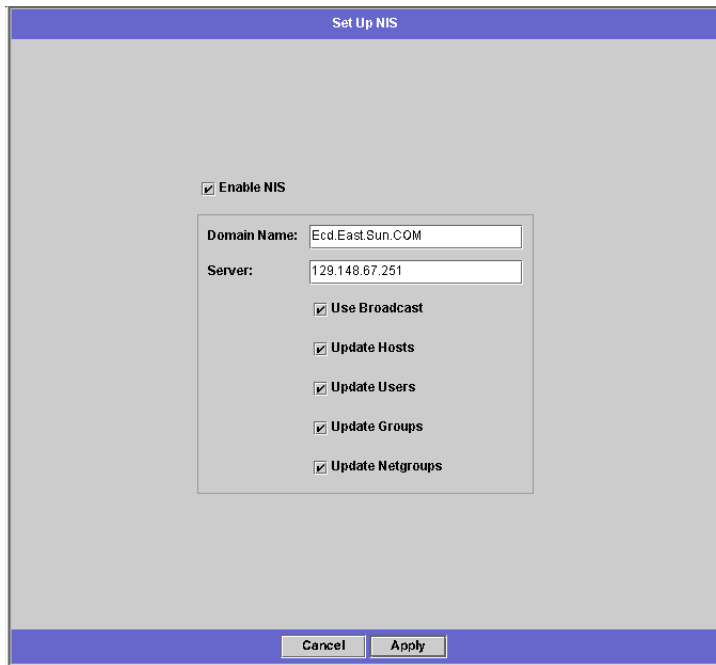
## Setting Up NIS

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

The **Set Up NIS** panel allows you to enable NIS and specify the domain name and server IP address.

To set up NIS:

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



**FIGURE 2-14** The Set Up NIS Panel

2. Select the **Enable NIS** checkbox. Enabling NIS configures the Sun StorEdge 5310 NAS Appliance to import the NIS database for host, user, and group information.
3. Enter 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. Enter 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. Select the **Use Broadcast** checkbox to automatically acquire the NIS server IP address.
6. Select the **Update Hosts** checkbox to download host information from the NIS server to the Sun StorEdge 5310 NAS Appliance server.
7. Select the **Update Users** checkbox to download user information from the NIS server to the Sun StorEdge 5310 NAS Appliance server.

8. Select the Update Groups checkbox to download group information from the NIS server to the Sun StorEdge 5310 NAS Appliance server.
9. Select the Update Netgroups checkbox to download netgroup information from the NIS server to the Sun StorEdge 5310 NAS Appliance server.
10. 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.

---

To set up NIS+:

1. For the Sun StorEdge 5310 NAS Appliance to function correctly in an NIS+ environment, you must add the Sun StorEdge 5310 NAS Appliance to the host credential file on the NIS+ server. Complete the following steps at your NIS+ server:

- a. Log in as root.

- b. Enter the following command:

```
nisaddcred -p unix.SERVER@DOMAIN -P SERVER.DOMAIN. des
```

where *SERVER* is the name of the Sun StorEdge 5310 NAS Appliance server, and *DOMAIN* is the name of the NIS+ domain that the Sun StorEdge 5310 NAS Appliance 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 StorEdge 5310 NAS Appliance is named **SS1**, and its NIS+ domain is **sun.com**, enter:

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

- c. You are prompted for a password. This password is also used later in this procedure for configuring the Sun StorEdge 5310 NAS Appliance to use NIS+. Enter the password.
2. From a remote client, open a Web browser window to the Sun StorEdge 5310 NAS Appliance server and log into Web Administrator.



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

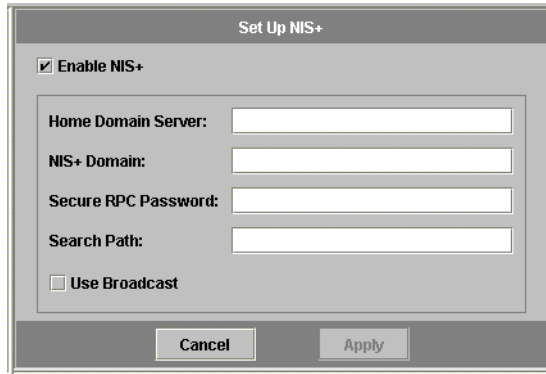


FIGURE 2-15 The Set Up NIS+ Panel

4. Select the Enable NIS+ checkbox.
5. 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 Sun StorEdge 5310 NAS Appliance automatically acquires the appropriate IP address for the home domain server.

6. In the NIS+ Domain field, enter the NIS+ home domain.

---

**Note** – NIS+ domain names must end with a period (“.”).

---

7. Enter the Secure RPC Password for the NIS+ server. This is the password that was set during Step 1c. on page 38.
8. 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, Sun StorEdge 5310 NAS Appliance first searches **eng.sun.com.** then **sun.com.**, and so on, when resolving names. Conversely, if you specify a search path like **sun.com.**, Sun StorEdge 5310 NAS Appliance searches only the domain **sun.com** when resolving names.

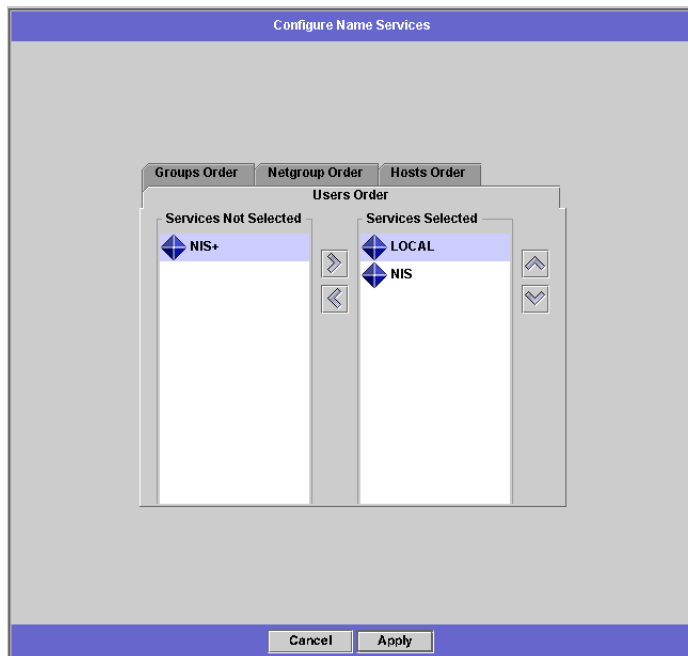
9. Select the Use Broadcast checkbox if you do not know the IP address of the home domain server (see step 5).
10. Click Apply to save your settings.

# 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 > Configuring Name Services**.



**FIGURE 2-16** The Configure Name Services Panel

2. Select the order of user lookup in the **Users Order** tab:
  - a. Select a service to be used in user lookup from the **Services Not Selected** box.
  - b. Click the  button to move it to the **Services Selected** box.
  - c. Repeat this process for each service used in user lookup.
  - d. To remove a service from user lookup, select it and click the  button.

- e. Then arrange the order of lookup services in the Services Selected box by selecting each service.
  - f. Click the  and  buttons to move it up or down. The service at the top of the list is used first in user lookup.
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 Notification

Set the SMTP (Simple Mail Transfer Protocol) server name and email notification recipients in this screen. When the system detects an error, the Sun StorEdge 5310 NAS Appliance 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 "Configuring Hosts" on page 99) or set up DNS (see "Setting Up DNS" on page 34).

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

1. In the navigation panel, select **Monitoring and Notification > Set Up Email Notification**.

The screenshot shows a window titled "Set Up Email Notification". It features two text input fields: "SMTP Server Name:" and "Email Address:". Below these are two checkboxes: "Notification" and "Diagnostics". A table labeled "List" has columns for "Recipient", "Notification", and "Diagnostics". To the right of the table are icons for adding (+) and removing (-) entries. Below the table is a "Notification Level" section with three radio buttons: "Errors", "Errors and Warnings" (which is selected), and "None". At the bottom of the window are "Cancel" and "Apply" buttons.

**FIGURE 2-17** The Set Up Email Notification Panel

2. Enter the name of the SMTP server which you want to use to send notification.
  3. Enter the email address of a person you want to automatically notify of system errors in the Email Address box.
  4. Specify the types of email for this recipient. Check Notification, Diagnostics, or both.
  5. Click  to add the new recipient to the List of recipients. Repeat steps 1. - 4. for all recipients. You may enter a maximum of four email addresses.
- To remove someone from the list, select the address and click .
6. **Select the Notification Level.**
    - Click the **Errors and Warnings** checkbox to notify recipients of all warnings and errors.
    - Click **Errors Only** to notify email recipients of errors, but not warnings.
    - Click **None** to disable notification.
  7. **Click Apply to save your settings.**

---

# Setting Up Logging

Enabling remote logging lets the Sun StorEdge 5310 NAS Appliance send its system 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 DNS settings on the Sun StorEdge 5310 NAS Appliance server 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. When it first starts up, the Sun StorEdge 5310 NAS Appliance creates a temporary log file in volatile memory to retain any errors that might occur during initial startup.

---

To set up remote and local logging:

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

The screenshot shows the 'Set Up Logging' dialog box. It is titled 'Set Up Logging'. There are two main sections: 'Enable Remote Syslogd' and 'Enable Local Log'.  
Under 'Enable Remote Syslogd':  
- 'Server:' text field contains '192.168.75.98'.  
- 'Facility:' dropdown menu is set to 'daemon'.  
- Eight checkboxes are checked: emergency, alert, critical, error, warning, notice, info, and debug.  
Under 'Enable Local Log':  
- 'Local File:' text field contains '/test/logfile'.  
- 'Archives:' text field contains '9'.  
- 'Size:' text field contains '999999'.  
At the bottom are 'Cancel' and 'Apply' buttons.

FIGURE 2-18 The Set Up Remote Logging Panel

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 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. *All messages sent to the syslogd server will have this facility value.* The possible facility values in the Set Up Remote Logging panel 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.

#### 5. Select the type of system events the Sun StorEdge 5310 NAS Appliance logs by placing a check mark on the type of event (see "System Events" on page 160).

#### 6. Check the Enable Local Log option to maintain a local log file.

#### 7. Enter the log file's path (the directory on the Sun StorEdge 5310 NAS Appliance where you want to store the log file) and filename in the Log File field.

#### 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 1000 to 999,999 kilobytes.

#### 10. Click Apply to save your settings.

---

## Assigning the Language

The Sun StorEdge 5310 NAS Appliance operating system supports Unicode, officially known as the Unicode Worldwide Character Standard. 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 select the language in which system commands, reports, and prompts are displayed:

1. In the navigation panel, select System Operations > Assign Language.



**FIGURE 2-19** The Assign Language Panel

2. Select a language for the Sun StorEdge 5310 NAS Appliance from the languages displayed in the drop-down list.
3. Click Apply to save your changes.

---

## Where to Go from Here

At this point, your Sun StorEdge 5310 NAS Appliance 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. The next chapter, "Initial File System Setup" on page 47, describes the initial setup of a file system. It does not cover all of the possible functions of the file system.

To set up quotas, shares, exports, or other access controls, see "Shares, Quotas, and Exports" on page 109 for detailed instructions. If there is a specific function you want to set up, look it up in the index to find the instructions.





## Initial File System Setup

---

This chapter covers initial file system setup. However, it does not cover all of the file system functions of the Sun StorEdge 5310 NAS Appliance. If there is a feature that you want to set up that is not described in this chapter, look it up in the index to find the instructions.

The Sun StorEdge 5310 NAS Appliance combines and simplifies the process of establishing the file system. Because some of the processes have been combined to simplify them, some of the terminology can be confusing. File system concepts are described below.

---

## File System Concepts

The following paragraphs provide definitions of some of the basic file system concepts and attributes used in the following discussions. Familiarize yourself with these terms.

### RAID

RAID stands for 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 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 looks exactly like a single drive. From the perspective of the system administrator, the physical component of the RAID is a group of drives, but the RAID itself can be administered as a single unit. There are multiple types of RAID configurations, and the Sun StorEdge 5310 NAS Appliance supports RAID 5.

## RAID 5

The 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.

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.

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 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 fault tolerance 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 six drive (5+1) RAID 5 groups plus two global hot spares. All subsequent EU F or EU S enclosures contain either one or two seven drive (6+1) RAID 5 groups for a total of seven or fourteen 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.

---

## LUN

LUN stands for Logical Unit Number and identifies the logical representation of a physical or virtual device. The Sun StorEdge 5310 NAS Appliance manages LUNs as independent entities. The Sun StorEdge 5310 NAS Appliance treats the LUN as a single storage volume.

LUNs are prebuilt on each Sun StorEdge 5300 RAID EU controller array and EU expansion enclosure.

# Partition

Partitions are sections on a LUN and provide a way to subdivide the total space available within a LUN. The Sun StorEdge 5310 NAS Appliance operating system supports 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 "Segment" on page 50). 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 allows 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 may be adding drives and LUNs, all that the user sees is that there is more space within the volume.

# File Volume

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 GB in size. To create a larger file volume, you can create and attach up to 63 segments (see *Segment* below) 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 units. However, the physical aspect is invisible to the user. All the user sees is more storage space within the volume.

# Segment

Segments are “volumes” of storage space created much like file volumes and 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 and, once attached to the original file volume, the different physical storage locations are invisible to the user. Therefore space can be added at need, without bringing down the network to restructure the data storage and create a bigger file volume.

---

## Establishing a File System

Establishing a file system requires three fundamental steps.

1. Establish the hardware configuration.
2. Define the software configuration.
3. Create a file system.

In the Sun StorEdge 5310 NAS Appliance, many of the tasks associated with these steps are automatically performed, greatly simplifying the task of creating functional storage space from new disks.

RAID sets (LUNs) are prebuilt on each Sun StorEdge 5300 RAID EU controller array and EU expansion enclosure and cannot be changed. If you need help, contact your Sun service representative for more information.

You will need to create file volumes to use these LUNs for Sun StorEdge 5310 NAS Appliance storage. Refer to "Creating a File Volume or a Segment" on page 50 for details.

## Creating a File Volume or a Segment

New file volumes are limited to 255 GB in size. To create a larger file volume, you can add up to sixty-three (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 segment(s) to the primary volume to increase its size.



---

**Caution – Sun StorEdge 5310 Cluster users**—Each head manages its own LUNs. Be sure to access the correct head for which you want to create a file volume. You should enable and configure failover before creating volumes and segments. Refer to "Enabling Failover" on page 24 for details.

---

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

## Create a File Volume or Segment Using the Create File Volume Panel

1. In the navigation panel, select File Volume Operations > Create File Volumes.

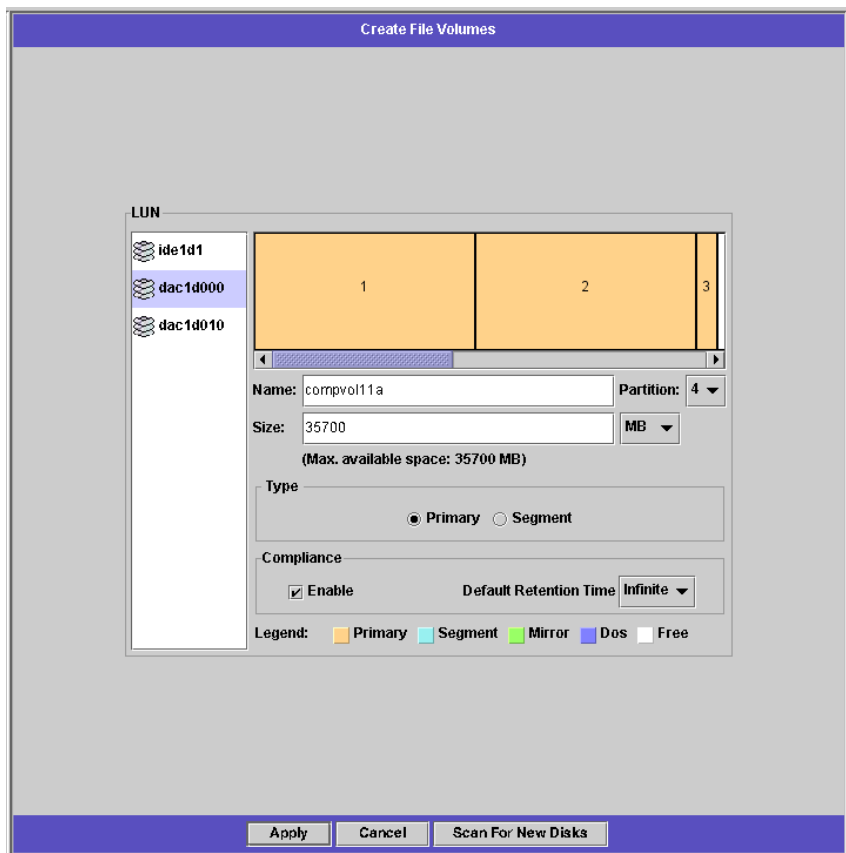


FIGURE 3-1 The Create File Volumes Panel

2. In the LUN box, click the LUN on which you want to create the primary file volume.

The partition number for the file volume in the **Partition** drop-down list 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) and “\_” (underscore) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a-z, A-Z).

4. Select whether the size of the file volume is reported in MB (megabytes) or GB (gigabytes) by clicking on the drop-down list.

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, in the Compliance section click Enable. See "Compliance Archiving Software" on page 152.



---

**Caution** – Once you enable compliance archiving on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled.

---

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

## Create a File Volume or Segment Using the System Manager

1. Right-click System Manager in the Navigation Panel.

2. Click Create Volume... or Create Segment... on the pop-up menu to open the desired dialog box.

3. In the LUN box, click the LUN on which you want to create the primary file volume.

The partition number for the file volume in the **Partition** drop-down list 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) and “\_” (underscore) 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 drop-down list.

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, in the Compliance section click Enable. See "Compliance Archiving Software" on page 152.



---

**Caution** – Once you enable compliance archiving on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled.

---

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

## Attaching Segments to a Primary File Volume

Attaching segments to a primary file volume expands its size. The segment becomes permanently associated to the volume and cannot be removed. In other words, the process cannot be reversed. You must create a segment before you can attach it to a volume. Refer to "Creating a File Volume or a Segment" on page 50 for instructions.



---

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

---

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

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



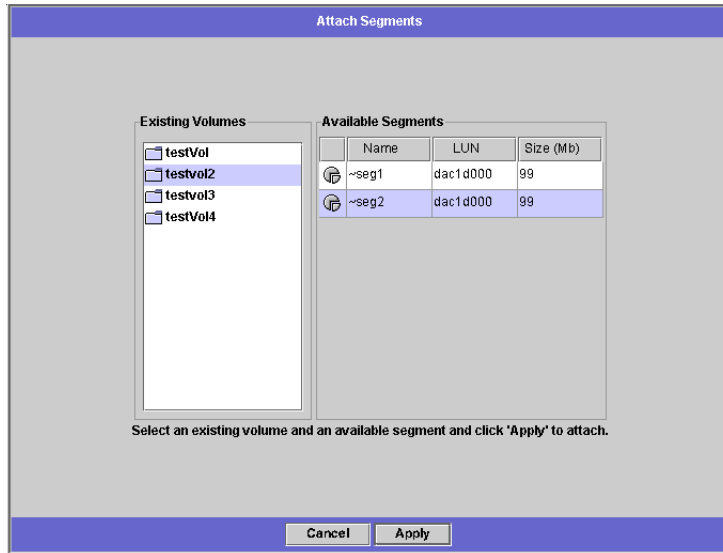
---

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

---

## *Attach a Segment Using the Attach Segments Panel*

1. Access the Attach Segments panel by clicking **File Volume Operations > Attach Segments**.



**FIGURE 3-2** The Attach Segments Panel

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.



## Attach a Segment Using the System Manager

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 Segment... .

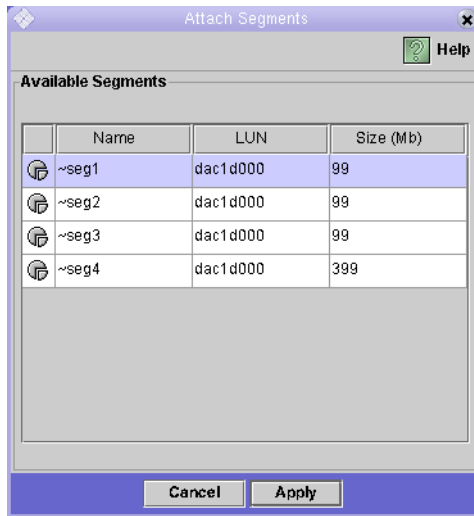


FIGURE 3-3 Available Segments

3. Click to select the desired segment. Only one segment can be selected and attached at a time.
4. Click Apply to attach the selected segment. Repeat Steps 3 and 4 to attach more segments.

---

## Where to Go from Here

At this point, your file system is 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, "System Management" on page 57.

Monitoring functions, which are essential to managing resources, are covered in Chapter 11, "Monitoring" on page 155. Maintenance functions like backup and restore are covered in Chapter 12, "System Maintenance" on page 179.



# System Management

---

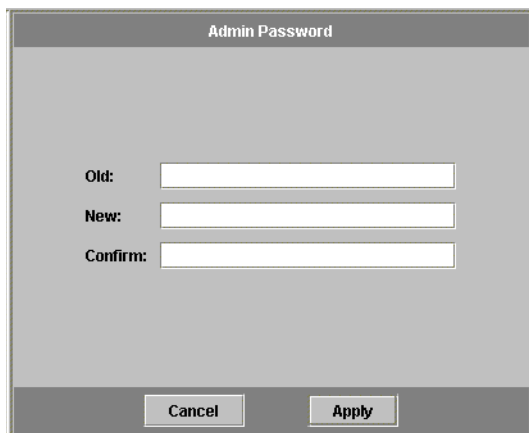
This chapter describes several basic system management functions. Many of these functions are primarily used only during initial system setup. However, they are available if you ever need to reset them.

---

## Setting the Administrator Password

To set the administrator password:

1. In the navigation panel, select **System Operations > Set Administrator Password**.



The screenshot shows a dialog box titled "Admin Password". It contains three text input fields labeled "Old:", "New:", and "Confirm:". At the bottom of the dialog, there are two buttons: "Cancel" and "Apply".

**FIGURE 4-1** The Admin Password Panel

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 21 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

Controlling the time and date on the Sun StorEdge 5310 NAS Appliance is essential for controlling file management. This section describes the functions available to maintain the correct time and date on the Sun StorEdge 5310 NAS Appliance.

---

**Note** – The first time you set the time and date on the Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance supports two types of time synchronization; Network Time Protocol (NTP) protocol or RDATE time protocol. You can configure the Sun StorEdge 5310 NAS Appliance 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 allow you to synchronize Sun StorEdge 5310 NAS Appliance server time with RDATE server time.

A third “method”, called manual synchronization, disables time synchronization. In this method, the system administrator sets the Sun StorEdge 5310 NAS Appliance 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**.

	NTP Server:	Auth Type:	Key ID:
<input checked="" type="checkbox"/> Enable Server 1	ntp-server	Symmetric Key	0
<input type="checkbox"/> Enable Server 2		None	

Min Poll Rate: 6  
Max Poll Rate: 10

Enable Broadcast Client  
 Require Broadcast Server Authentication

RDATE Synchronization

RDATE Server:   
Tolerance: 180

Cancel Apply

FIGURE 4-2 The Set Up Time Synchronization Panel

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**—If you want to use NTP synchronization and have at least one NTP server on the network, select this option button and complete the following:
    - **Enable Server 1**—To enable an NTP server, select the **Enable Server 1** checkbox and enter the information in the corresponding fields. Do the same with a second NTP server if you want. You can configure up to two NTP servers.

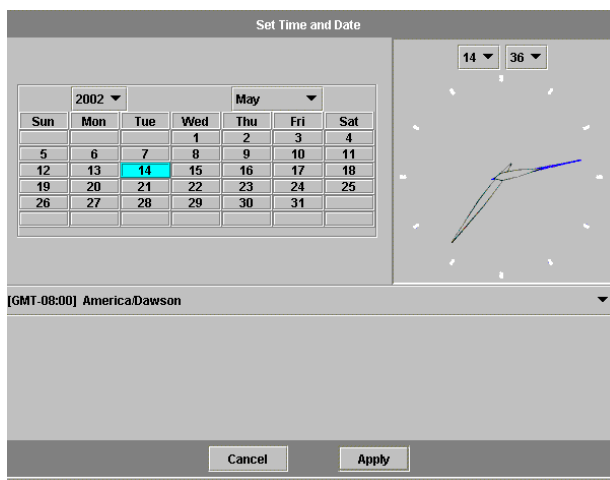
- **Enable Server 2**—To enable a second, or alternate, NTP server, select the **Enable Server 2** checkbox and enter the information in the corresponding fields. You can configure up to two NTP servers.
- **NTP Server**—Enter the name or IP address of the NTP server the Sun StorEdge 5310 NAS Appliance will poll for the current time.
- **Auth Type**—Authentication support allows the Sun StorEdge 5310 NAS Appliance to verify that the server is known and trusted by using a key and key identifier. The NTP server and the Sun StorEdge 5310 NAS Appliance must agree on the key and key identifier to authenticate their messages. Choose the type of authentication you want to use, either **None** (do not use an authentication scheme) or **Symmetric Key**.
- **Key ID**—If you selected **Symmetric Key** as the authorization scheme in the previous field, enter the key identifier for this NTP server. The valid range for this value is **1** to **65534**.
- **Min Poll Rate**—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** means poll events occur at least 16 seconds apart. The valid range for this field is **4** to **17**.
- **Max Poll Rate**—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** means that poll events occur no more than 16 seconds apart. The valid range for this field is **4** to **17**, but must be larger than the minimum polling interval.
- **Enable Broadcast Client**—Select this checkbox for the Sun StorEdge 5310 NAS Appliance to respond to server broadcast messages received on any interface. This function is intended for configurations involving one or a few NTP servers with a large number of clients requiring time synchronization from those servers.
- **Require Broadcast Server Authentication**—Select this checkbox to require the NTP client to verify that a server which has broadcast messages to the Sun StorEdge 5310 NAS Appliance is a known and trusted server.
- **RDATE Synchronization**—To set up the RDATE server and tolerance window, select this checkbox and enter the following:
  - **RDATE Server**—Enter the name or IP address of the RDATE server.
  - **Tolerance**—Enter the maximum tolerance allowed for the time received from the RDATE server, from **0** to **3600** seconds. If the Sun StorEdge 5310 NAS Appliance server time is different than the RDATE server time by less than this number of seconds (+ or -), the Sun StorEdge 5310 NAS Appliance server time is synchronized with the RDATE server time. If there is a larger discrepancy, Sun StorEdge 5310 NAS Appliance server time is not automatically synchronized with the RDATE server. This check occurs every day at 11:45 PM.

### 3. Click **Apply** to save your changes.

# Setting the Time and Date Manually

To set the time and date for the Sun StorEdge 5310 NAS Appliance server:

1. In the navigation panel, select **System Operations > Set Time and Date**.



**FIGURE 4-3** The Set Time and Date Panel

2. Select the correct year from the drop-down list box above the calendar and to the left.
3. Select the correct month from the drop-down list 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 drop-down list box above the clock and to the right.
7. Select the correct time zone from the drop-down list at the bottom of the screen. Selecting the correct time zone allows the Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance, this will set the secure clock to the same time and date. Make sure you set the time and date accurately as you can only set the secure clock once.

---





## Managing System Ports

---

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.

---

### Sun StorEdge 5310 NAS Appliance Port Locations

The Sun StorEdge 5310 NAS Appliance identifies ports in a predefined order based on their type and their physical and logical location on the server. Refer to your *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide* to identify the port locations for your Sun StorEdge 5310 NAS Appliance.

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

- **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 head (head 2) holds the 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 head. The partner IP address is held as a backup alias IP address by the primary 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 was still active.

---

**Note** – At least one port on each head 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 StorEdge 5310 Cluster system 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 "Sun StorEdge File Replicator" on page 136.
- **Private**—**Sun StorEdge 5310 Cluster 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

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.

Single-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 could provide up to 20 usable IP addresses.

On a Sun StorEdge 5310 Cluster system, 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 head. In the event of head failover, the healthy head activates these reserved backup IP addresses, allowing network access to continue with minimal interruption. See "About Head Failover" on page 24 for details on head failover.

For dual-head systems, you can only add alias IP addresses to ports that are assigned a **primary** role. The role options are described in "Sun StorEdge 5310 NAS Appliance Port Locations" on page 63.

---

**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 StorEdge 5310 Cluster system. 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.

---

---

# Configuring Network Ports

For a description of how to configure network ports, refer to "Configuring the Network Ports" on page 27.

---

## Port Bonding

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

A Sun StorEdge 5310 NAS Appliance system may have up to four (4) bonds of any type. Each bond may have up to six (6) ports.

## 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.

---

# High Availability Bonds

High availability (HA) port bonding provides port failover capabilities to the Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance services to continue without any interruptions.

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-Head System

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

You can bond ports after configuring them. However, alias IP addresses and some other aspects of the original configurations may change. After you create a port bond, return to "Configuring Network Ports" on page 65 to configure the port bond. Once 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-head system:

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

Bond ID	Type	Status	IP Address	Subnet Ma...	Broadcast ...	Slaves
bond1	Port Aggregati...	Normal	129.148.67.16	255.255.255.0	129.148.67.255	emc1 emc2

Buttons: Create, Edit, Remove, Recover

FIGURE 5-1 The Bond NIC Ports Panel

2. Click Create.

Create Port Bond

IP Address: 10 . 8 . 120 . 110

Subnet Mask: 255 . 255 . 255 . 0

Broadcast Address: 10 . 8 . 120 . 255

Partner Ip Address: . . .

Port Aggregation

High Availability



Available NIC Ports:

- emc1 (Intel Gigabit Copper)
- emc2 (Intel Gigabit Copper)
- emf3 (Intel Gigabit Fiber)
- emf4 (Intel Gigabit Fiber)

NIC Ports in This Bond:

Buttons: Apply, Cancel

FIGURE 5-2 The Create Port Bond Dialog Box

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** box, 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 Ports" on page 65.

## Bonding Ports on a Sun StorEdge 5310 Cluster System

To bond ports on dual-head systems, you only need to complete the following procedure on one head. 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 IP addresses and some other aspects of the original configurations may change. After you create a port bond, return to "Configuring Network Ports" on page 65 to configure the port bond.

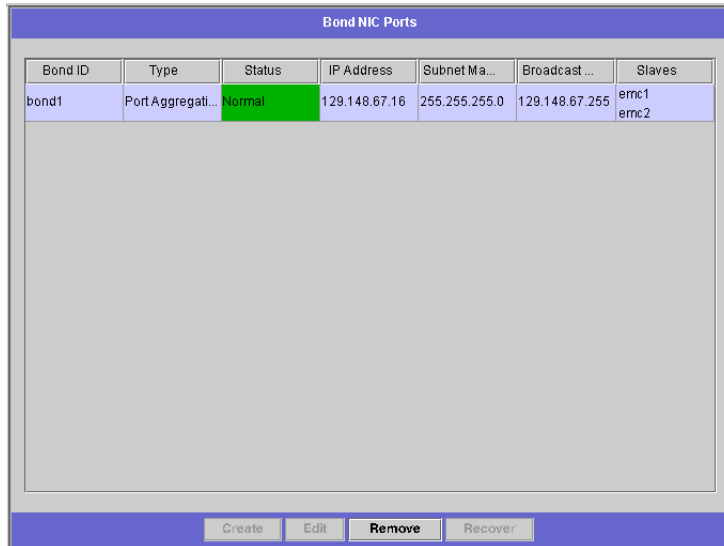
For more information on dual-head port bonding, see the "Example of Dual-Head Port Bonding" on page 70.

---

**Note** – You can use only ports with a **Primary** role for port bonding. For more information about port roles, see "Sun StorEdge 5310 NAS Appliance Port Locations" on page 63.

---

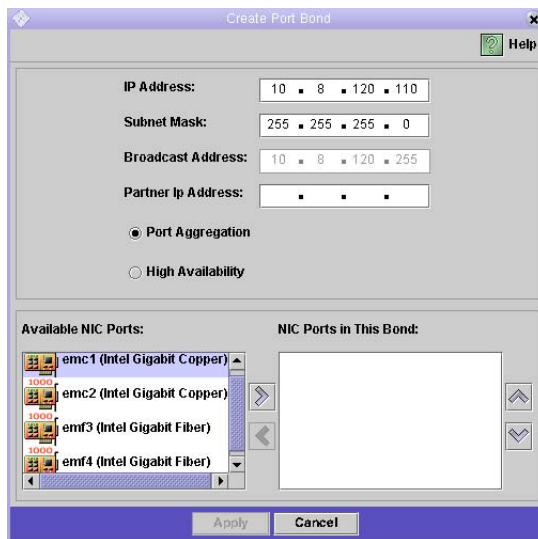
1. In the navigation panel, select Network Configuration > Bond NIC Ports.



Bond ID	Type	Status	IP Address	Subnet Ma...	Broadcast ...	Slaves
bond1	Port Aggregati...	Normal	129.148.67.16	255.255.255.0	129.148.67.255	emc1 emc2

FIGURE 5-3 The Bond NIC Ports Panel

2. Click Create.



IP Address: 10 . 8 . 120 . 110

Subnet Mask: 255 . 255 . 255 . 0

Broadcast Address: 10 . 8 . 120 . 255

Partner IP Address: . . .

Port Aggregation

High Availability

Available NIC Ports: emc1 (Intel Gigabit Copper), emc2 (Intel Gigabit Copper), emf3 (Intel Gigabit Fiber), emf4 (Intel Gigabit Fiber)


NIC Ports in This Bond:

FIGURE 5-4 The Create Port Bond Dialog Box

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

4. Select a port, then clicking  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 head, 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 Head 1, Ports 2 and 3 on Head 2 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 Ports" on page 65. Once you bond two or more ports, you cannot add IP aliases to the individual ports, only to the bond.

## Example of Dual-Head Port Bonding

FIGURE 5-5 shows an example of a Sun StorEdge 5310 Cluster system connected to two different subnets. To show all possible combinations, this example shows each head having a **heartbeat** port and four additional ports. All ports except the heartbeat port on each head are configured with a **Primary** role.

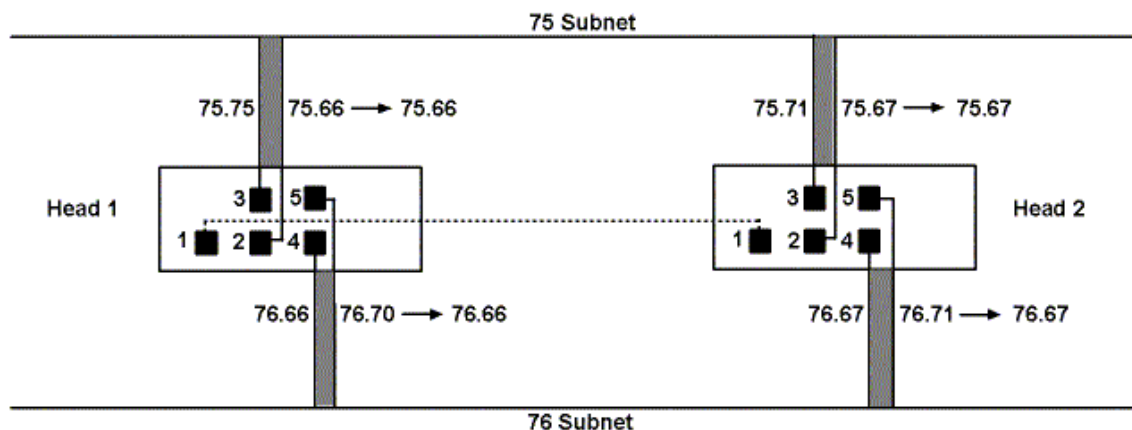


FIGURE 5-5 Dual-Head Port Bonding



If Ports 2 and 3 are bonded, and Ports 4 and 5 are bonded, the following IP configuration results:

**TABLE 5-1** Dual-Head Port Bonding Example

Head	Ports to be Bonded		Port Bond		
	Name	Primary IP Address	Name	Primary IP Address	Backup IP Address
1	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
	Port 5	192.1xx.76.70			
	Port 2	192.1xx.75.67			
2	Port 3	192.1xx.75.71	Bond 1	192.1xx.75.67	192.1xx.75.66
	Port 4	192.1xx.76.67			
	Port 5	192.1xx.76.71	Bond 2	192.1xx.76.67	192.1xx.76.66

The primary IP address of each port on Head 1 is the backup IP address for the corresponding port on Head 2, and vice versa.

In the event of head failover, the surviving head activates the IP addresses of the failed head. 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 64.



# File System Management

---

This chapter describes Sun StorEdge 5310 NAS Appliance file system management tasks beyond those described in Chapter 3, “Initial File System Setup.”

---

## LUN Management

### Rebuilding a LUN

If one of the drives in a LUN fails, the LED on that drive turns steady yellow. LUN rebuilding occurs automatically if a drive in the Sun StorEdge 5310 NAS Appliance is specified as a hot spare. 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 the *Sun StorEdge 5310 NAS Appliance Hardware User Guide* for information on replacing a failed drive.

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

# File Volume and Segment Management

## Editing File Volume Properties

---

**Note** – Regular (non-compliance) volumes cannot have compliance archiving enabled. Compliance-enabled volumes cannot be renamed or have compliance archiving disabled.

---

To rename a volume, enable checkpoints, or enable quotas:

1. In the navigation panel, select **File Volume Operations > Edit Properties**.

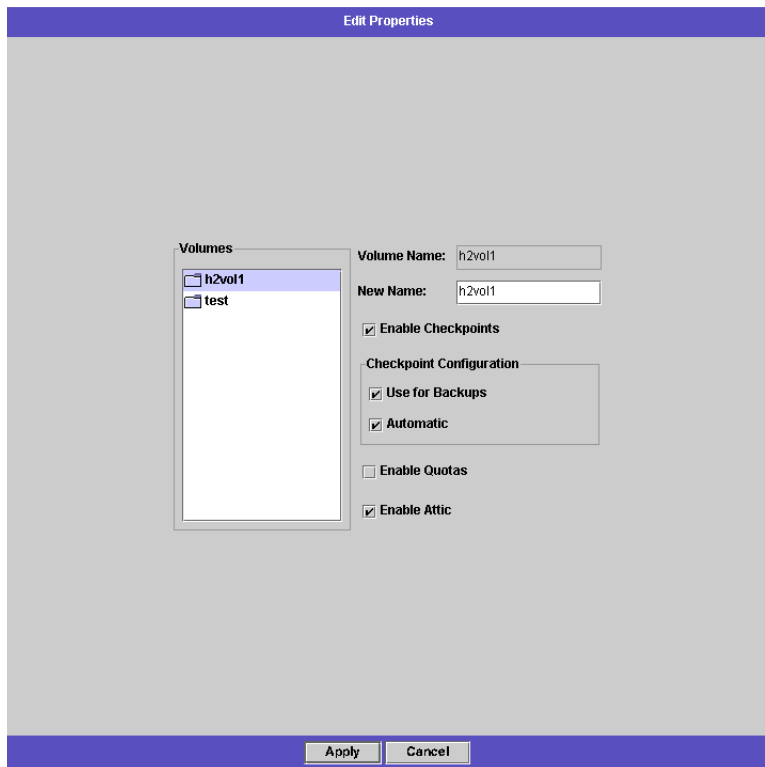


FIGURE 6-1 The Edit Properties Panel

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) and "\_" (underscore) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a-z, A-Z).

4. Select either or both of the following options for this volume:

- **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 unchecking this checkbox.

5. Click **Apply** to save your changes.

## Deleting File Volumes

---

**Note** – Compliance-enabled volumes cannot be deleted.

---

To delete a file volume or segment:

1. In the navigation panel, select File Volume Operations > Delete File Volumes.

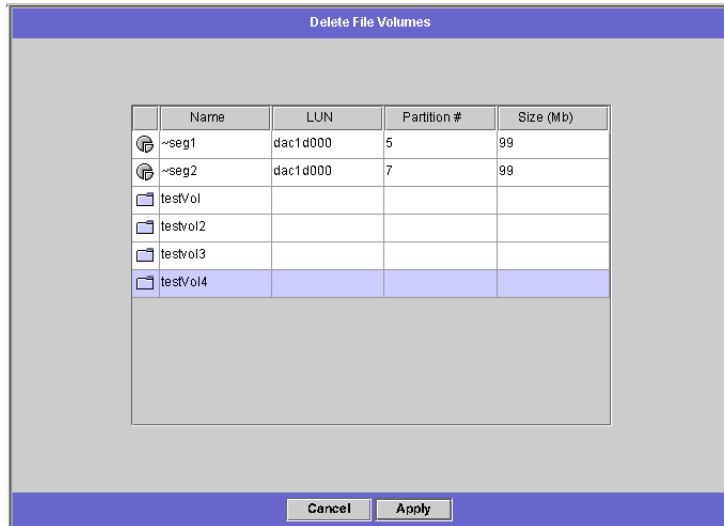


FIGURE 6-2 The Delete File Volumes Panel

2. Select the file volume or segment you want to delete.
3. Click Apply.

## Managing File Deletion and Checkpoints

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, refer to page 75.)

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 File Checkpoints" on page 195 for instructions on removing checkpoints.

# Viewing Volume Partitions

The View Volume Partitions panel is a read-only display of the LUNs defined for the Sun StorEdge 5310 NAS Appliance.

To view volume partitions:

1. In the navigation panel, select **File Volume Operations > View Volume Partitions**.

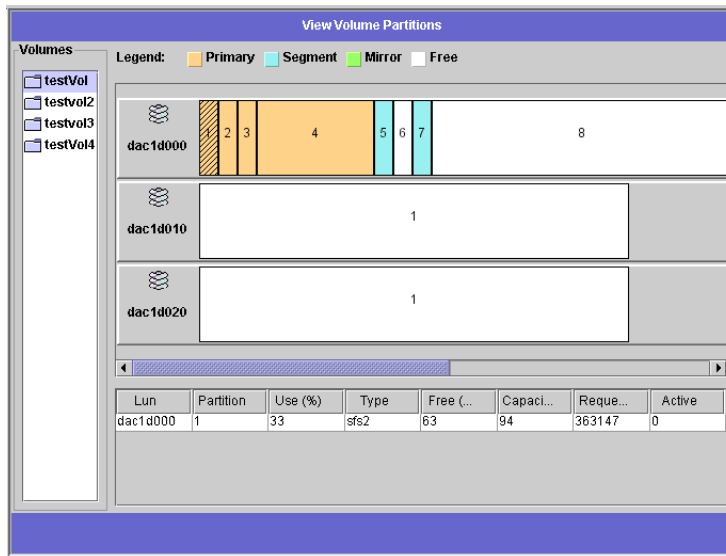


FIGURE 6-3 The View Volume Partitions Panel

2. In the Volumes list, select the file volume for which you want to view partitions.

The following information is shown for the selected volume:

- **LUN**—Lists all LUNs for the selected file volume.
- **Partition**—Shows partitions for the selected file volume.
- **Use**—Shows the percentage of the partition in use.
- **Type**—Shows the partition type as either sfs2 (primary) or sfs2ext (segment).
- **Free**—Shows the amount of unused space on the partition.
- **Capacity**—Shows the total size of the partition.
- **Requests**—Displays the total number of requests processed for the partition.
- **Active**—Displays the active requests that have not yet been processed for the partition.





## Name Services

---

The Sun StorEdge 5310 NAS Appliance 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 System (DNS, see "Setting Up DNS" on page 34). 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 Sun StorEdge 5310 NAS Appliance automatically performs ADS updates. See "Active Directory Services" on page 80 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 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 33 for more information.
- **DNS**—Domain Name System (DNS) resolves domain names to IP addresses for the Sun StorEdge 5310 NAS Appliance system. This service allows you to identify a server by either its IP address or its name. See "Setting Up DNS" on page 34 for more information.
- **NIS**—Network Information Service (NIS) configures the Sun StorEdge 5310 NAS Appliance to import the NIS database. It administers access to resources based on the users group and host information. See "Setting Up NIS" on page 36 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 38 for more information.

This chapter describes ADS services in detail, LDAP setup, and how to change name service lookup order. For setup instructions for WINS, DNS, NIS, and NIS+, refer to "Name Services" on page 30.

---

## Active Directory Services

For the Sun StorEdge 5310 NAS Appliance to integrate seamlessly into a Windows 2000 Active Directory environment, the following items must exist on the network:

- A Windows 2000 server domain controller
- An Active Directory-integrated DNS server allowing dynamic updates (needed in order to use the Sun StorEdge 5310 NAS Appliance Dynamic DNS capability) is recommended but not required for using ADS.

After setting up ADS, you can set ADS to publish specific Sun StorEdge 5310 NAS Appliance shares in the ADS directory. To do so, create or update Sun StorEdge 5310 NAS Appliance SMB shares and specify the share container for each share you want to publish.

# Setting Up ADS

To enable ADS service on the Sun StorEdge 5310 NAS Appliance:

1. In the navigation panel, select **System Operations > Set Time and Date**.

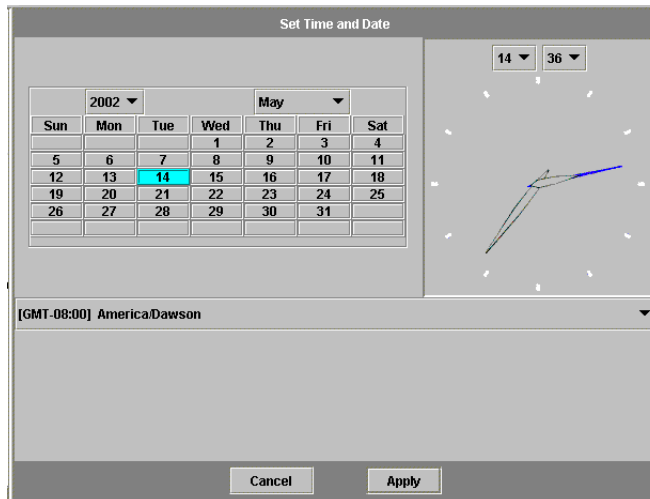


FIGURE 7-1 The Set Time and Date Panel

2. Verify that the Sun StorEdge 5310 NAS Appliance 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 that the Sun StorEdge 5310 NAS Appliance uses 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.

The screenshot shows a configuration window titled "Configure Domains and Workgroups". It has two main sections: "Domain" and "Workgroup". The "Domain" section is active, indicated by a selected radio button. It contains several input fields: "Domain:" with the value "WG4DOMAIN", "User Name:" with "admin", and "Password:" with masked characters. To the right, there is a checked checkbox for "Enable ADS". Below it, the "ADS Information" section includes "Container:" with "test" and an empty "Site:" field. The "Kerberos Domain Information" section has empty "Realm:" and "Server:" fields. The "Workgroup" section is inactive and contains an empty "Name:" field and a "Comments:" field with the text "Sun StorEdge 5210". At the bottom of the window are "Cancel" and "Apply" buttons.

FIGURE 7-2 The Configure Domains and Workgroups Panel

5. Select the Enable ADS checkbox.
6. In Domain, enter the Windows 2000 Domain in which ADS is running. The Sun StorEdge 5310 NAS Appliance 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**

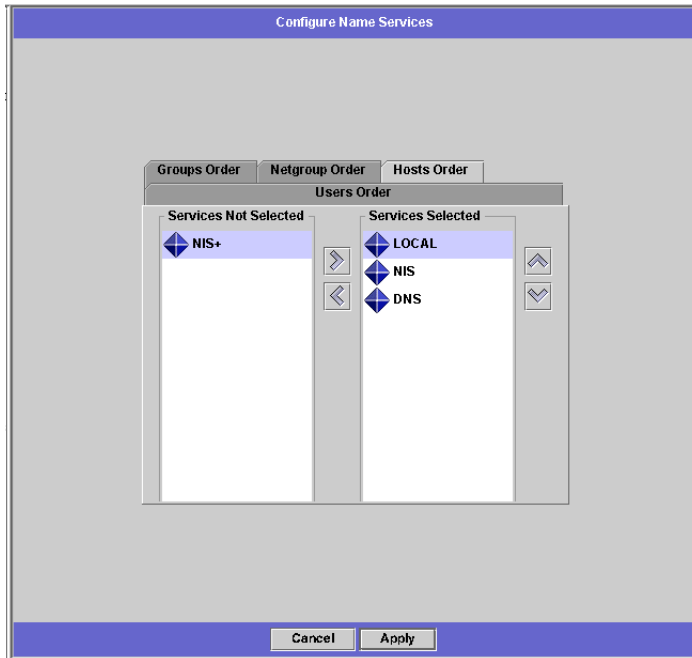
Do not include the domain name in the path.

- 10. In the Site field, enter the name of the local ADS site if different from the ADS domain. This field is usually left blank.**
- 11. In the Kerberos Realm Info section, enter the Realm name used to identify ADS. This is normally the ADS domain or the DNS domain. When you click Apply, this entry is converted to all upper-case letters.**
- 12. 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 Sun StorEdge 5310 NAS Appliance can locate the KDC server through DNS.**
- 13. Click Apply to save and invoke your changes.**

# Verifying Name Service Lookup Order

To verify name service lookup order:


1. Select **UNIX Configuration > Configure Name Services**.





**FIGURE 7-3** The Configure Name Services Panel

2. Verify that the name service lookup order for DNS is enabled and set to the correct priority.

- a. Select the **Hosts Order** tab. Be sure **DNS** service is listed under **Services**

Selected in the right-hand box. If it is not, select **DNS** service and click the  button.

- b. Use the  and  buttons to change the order in which the selected services are scanned.

3. Click **Apply** to save any changes.

## Verifying DNS Configuration

To verify that DNS is enabled and configured properly to support ADS:

1. In the navigation panel, select **Network Configuration > Configure TCP/IP > Set Up DNS**.

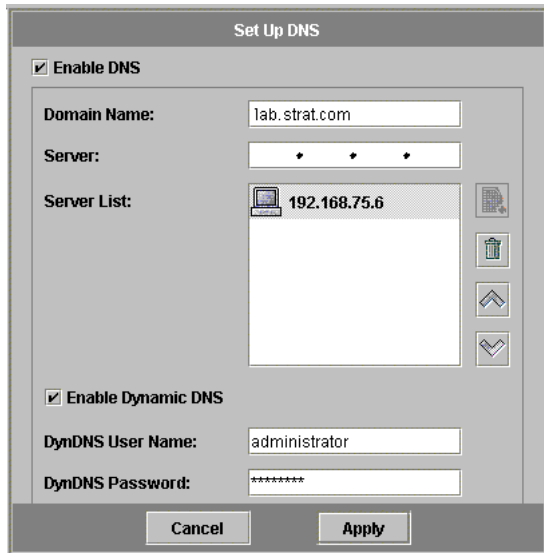



FIGURE 7-4 The Set Up DNS Panel

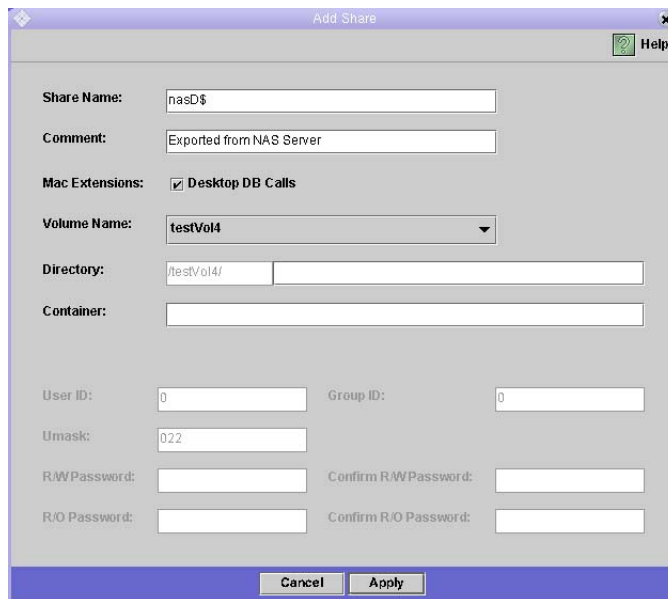
2. If DNS is not enabled, select the **Enable DNS** checkbox.
3. If you have not entered a domain name, enter the DNS Domain Name. This name must be the same as the ADS domain.
4. In the **Server** field, enter the IP address of the DNS server you want the Sun StorEdge 5310 NAS Appliance server to use. Then click  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 Sun StorEdge 5310 NAS Appliance 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 non-secure 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 Sun StorEdge 5310 NAS Appliance immediately updates DNS with its host name and IP address.

## Publishing Shares in ADS

To publish shares in ADS:

1. In the navigation panel, select **Windows Configuration > Configure Shares**.
2. Click **Add**.



The screenshot shows the 'Add Share' dialog box with the following fields and values:

- Share Name: nasD\$
- Comment: Exported from NAS Server
- Mac Extensions:  Desktop DB Calls
- Volume Name: testVol4
- Directory: /testVol4/
- Container: (empty)
- User ID: 0
- Group ID: 0
- Umask: 022
- R/W Password: (empty)
- Confirm R/W Password: (empty)
- R/O Password: (empty)
- Confirm R/O Password: (empty)

Buttons: Cancel, Apply

**FIGURE 7-5** The Add Share Dialog Box

3. Enter a Share Name.
4. Optionally, 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. In the Directory field, enter an existing directory on the selected volume that you want to share. This field is optional.



---

**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 83 for more information.
8. Click **Apply**. The share is added to the specified container.

---

**Note** – The container specified must already exist for the share to be published in that container. Sun StorEdge 5310 NAS Appliance does not create container objects in the ADS tree.

---

## Updating ADS Share Containers

To update the ADS container of a share:

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** dialog box.
4. Enter the new share container.
5. Click **Apply**. The Sun StorEdge 5310 NAS Appliance updates the share container.

## Removing Shares from ADS

To remove a share from the ADS directory:

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** dialog box.
4. Delete the share container from the **Container** field.
5. Click **Apply**.

---

# Setting Up LDAP

To use LDAP, the LDAP server must be running.

To enable LDAP service on the Sun StorEdge 5310 NAS Appliance:

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



The screenshot shows a web-based configuration interface for setting up NSSLDAP. The interface has a blue header bar with the text "Set Up NSSLDAP". Below the header is a large gray area containing a checkbox labeled "Enable NSSLDAP". Underneath the checkbox is a form with four input fields: "Domain (DN):", "Password:", "Server:", and "Proxy (DN):". The "Server:" field contains three asterisks. At the bottom of the gray area are two buttons: "Apply" and "Cancel".

**FIGURE 7-6** The Set Up NSSLDAP Panel

2. To enable LDAP, check the **Enable NSSLDAP** checkbox.
3. In the **Domain** field, enter the domain name of the LDAP server, e.g., *foo.com*.
4. In the **Password** field, enter the password set on the LDAP server.
5. In the **Server** field, enter the IP address for the LDAP server.
6. In the **Proxy** field, enter the proxy domain, depending on the server settings.
7. Click **Apply** to save the settings.

---

## Setting Up WINS

For instructions on setting up WINS, refer to "Setting Up WINS" on page 33.

---

## Setting Up DNS

For instructions on setting up DNS, refer to "Setting Up DNS" on page 34.

---

## Setting Up NIS

For instructions on setting up NIS, refer to "Setting Up NIS" on page 36.

---

## Setting Up NIS+

For instructions on setting up NIS+, refer to "Setting Up NIS+" on page 38.

---

## Changing Name Service Lookup Order

The Name Service (NS) lookup order controls the sequence in which the Sun StorEdge 5310 NAS Appliance 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 > Configuring Name Services.

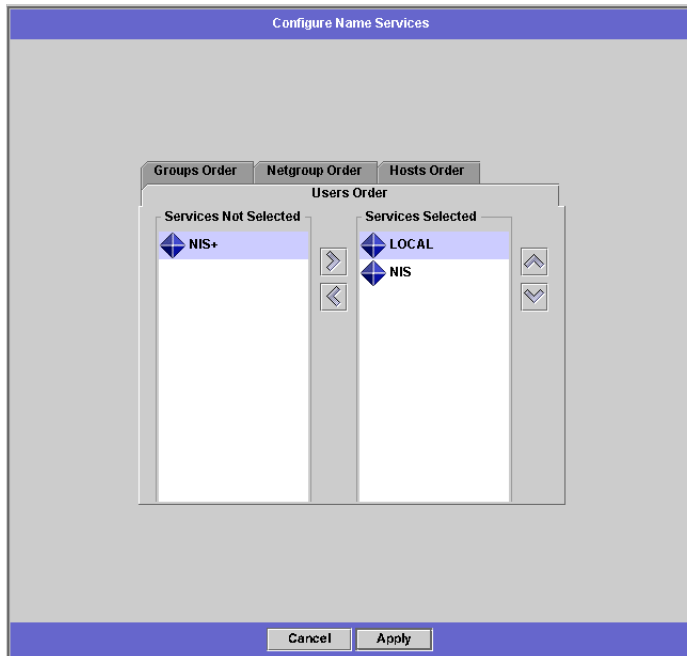






FIGURE 7-7 The Configure Name Services Panel

2. Click on the Users Order tab to select the order of user lookup.
  - a. Select a service from the Services Not Selected box.
  - b. Click  to move it to the Services Selected box. To remove a service from user lookup, select it and click .
  - c. Arrange the order of lookup services in the Services Selected box by selecting each service and clicking  and  to move it up or down. The service at the top of the list is used first in user lookup.
3. Click on the Groups Order tab to select the services to be used for group lookup, following the procedure in step 2.
4. Click on the Netgroup Order tab to select the services to be used for netgroup lookup, following the procedure in step 2.

5. Click on the Hosts Order tab to select the services to be used for hosts lookup, following the procedure in step 2.
6. Click Apply to save your changes.



## Group, Host, and File Directory Security

---

This chapter describes the various settings for local groups, hosts, user and group mapping, and file directory security on the Sun StorEdge 5310 NAS Appliance system.

To configure Windows security, refer to "Configuring Windows Security" on page 31.

---

## Sun StorEdge 5310 NAS Appliance Local Groups

### About Sun StorEdge 5310 NAS Appliance Local Groups and Privileges

The requirements for Sun StorEdge 5310 NAS Appliance built-in local groups are different from those of a Windows system. As a 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 CIFS networking.

---

Sun StorEdge 5310 NAS Appliance local groups are primarily used to manage resources and to perform backup related operations. There are three Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance built-in local group.

## Configuring Privileges for Sun StorEdge 5310 NAS Appliance 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 StorEdge 5310 NAS Appliance, 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 pre-defined operations. Privileges override or bypass object-level access rights.



The privileges supported on the Sun StorEdge 5310 NAS Appliance are shown in Table 8-1. 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 8-1** Sun StorEdge 5310 NAS Appliance 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/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 Sun StorEdge 5310 NAS Appliance local built-in groups are shown in Table 8-2. 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 8-2** Default Group Privileges

Group	Default Privilege
Administrators	Take ownership
Backup Operators	Backup and restore
Power Users	None

## Ownership Assignment

By default, the Domain Admins group of the domain that the Sun StorEdge 5310 NAS Appliance 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.

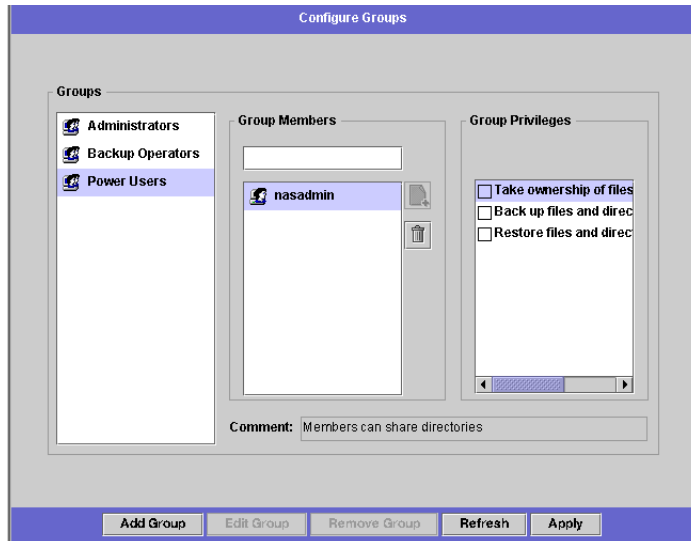
On Windows systems, the domain administrator membership of the local administrator group can be revoked. In such cases, members of the domain administrator group are treated as regular users. On the Sun StorEdge 5310 NAS Appliance, however, the domain administrator is always assigned membership of the local administrators group—however, the domain administrator is not listed as a member of this group, so you cannot revoke its membership. This difference between Windows and Sun StorEdge 5310 NAS Appliance is due to the nature of the NAS appliance. Because there are no local users, and thus no local Windows administrators, the domain administrator group must have administrative control on the Sun StorEdge 5310 NAS Appliance.

## Adding and Removing Group Members and Configuring Privileges

The **Configure Groups** panel lets you add any domain user to any of the three Sun StorEdge 5310 NAS Appliance local groups.

To add or remove a member of a group:

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



**FIGURE 8-1** The Configure Groups Panel

Existing members of the selected group are listed in the Group Members box.

2. To add a group, do the following:
  - a. Click Add Group.



**FIGURE 8-2** The Add Group Dialog Box

- b. In the Group field, enter the name of the group.
    - c. In the Comment field, enter a description of or comments about the group.
    - d. Click Apply to save your changes.
3. To remove a group, do the following:
  - a. Select the group you want to remove.
  - b. Click Remove Group.
  - c. Click Apply to save your changes.
4. To add or remove a group member, do the following:
  - a. Highlight the group to which you want to add or from which you want to remove members. Existing members for the selected group are listed in the Group Members box.
  - b. In the Group Members box highlight the member you want to add or delete, and click the Add or Delete icon.
  - c. Click Apply to save your changes.

## Configuring Privileges

The **Configure Privileges** panel allows administrators to view, grant, and revoke privileges from Sun StorEdge 5310 NAS Appliance groups.

To configure NT privileges:

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

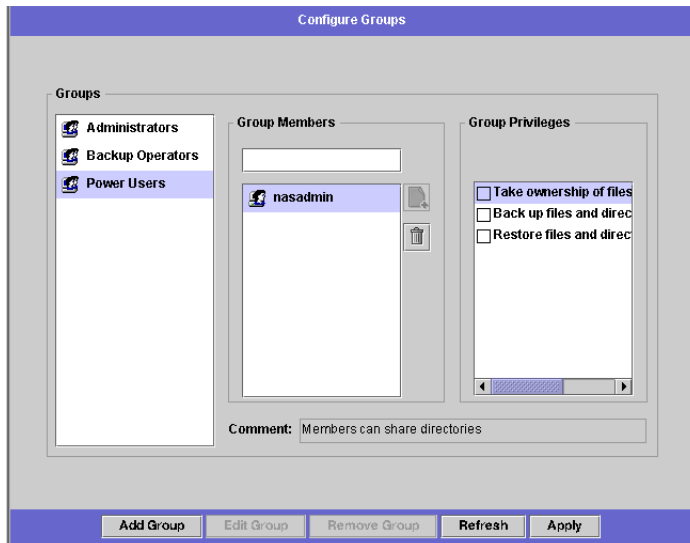


FIGURE 8-3 The Configure Groups Panel

2. In the **Groups** box, select the group for which you want to assign privileges.
3. In the **Group Privileges** box, click the check box for the privilege you want to grant to the group.
4. To revoke the privileges for a group, clear the check box for the privilege you want to revoke.
5. Click **Apply**.

---

# Configuring Hosts

The **Set Up Hosts** panel lets you add, edit, or remove entries from the system host file. The table shows current host information, including host name, host 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 Sun StorEdge 5310 NAS Appliance file system and have read and write access to all files and directories in that file system.

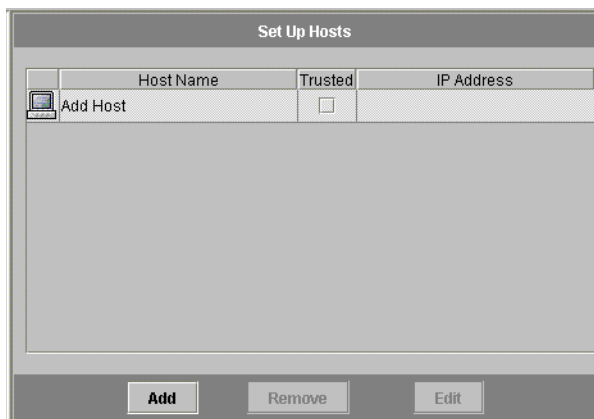
---

## Adding a Host

The **Set Up Hosts** panel lets you view host information and designate whether a host is trusted. A **root user** on an NFS client has root privileges on the Sun StorEdge 5310 NAS Appliance if that client was defined as a **trusted host** and has access to all files regardless of file permissions.

To manually add a host to the Sun StorEdge 5310 NAS Appliance server:

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



**FIGURE 8-4** The Set Up Hosts Panel

2. Click Add.

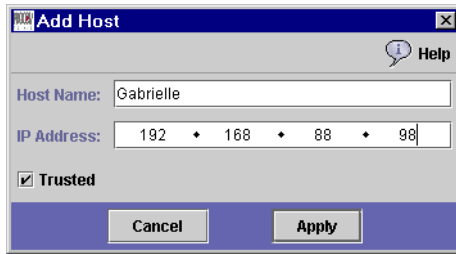


FIGURE 8-5 The Add Host Dialog Box

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. Enter the new host's IP Address.
5. If necessary, select the checkbox to assign the host Trusted status. A trusted host has root access to the Sun StorEdge 5310 NAS Appliance.
6. Click Apply to save your changes.

## Editing Host Information

To change the name, IP address, or trust status of a particular host:

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.

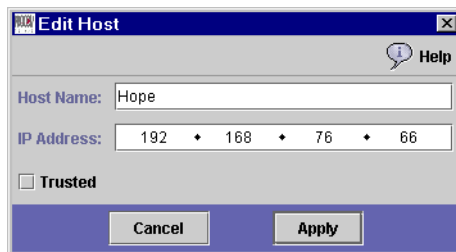


FIGURE 8-6 The Edit Host Dialog Box

**3. Revise the following information as needed:**

- **Host Name**—This is 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.
- **IP Address**—This is the host's IP address.
- **Trusted**—Select this checkbox to assign the host trusted status. Exercise caution in assigning trusted status to hosts.

**4. Click Apply to save your changes.**

## Removing a Host

To remove a host mapping from the Sun StorEdge 5310 NAS Appliance system 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.**

---

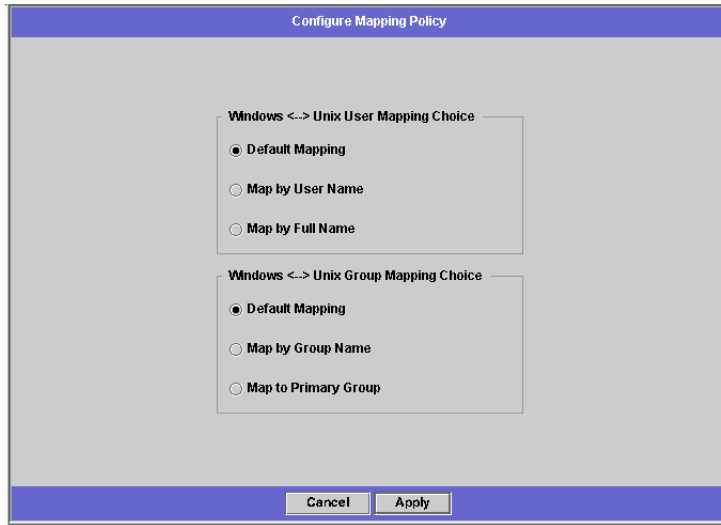
## Mapping User and Group Credentials

Sun StorEdge 5310 NAS Appliance servers are designed to reside in a multi-protocol 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.

User and group mapping is a mechanism to establish credential equivalence on the Sun StorEdge 5310 NAS Appliance to provide common access using either environment.

To define the mapping policy:

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



**FIGURE 8-7** The Configure Mapping Policy Panel

2. The **Windows <-> UNIX User Mapping Choice** section lets you determine the user mapping settings. Select one of the following:
  - **Default Mapping**—Select this option if there is no pre-defined mapping rule between Windows and UNIX users. New users will be assigned a newly-generated, unique ID by the system.
  - **Map by User Name**—Select this option to let the system map UNIX and Windows users who have identical user names, allowing the same user to access the Sun StorEdge 5310 NAS Appliance from both environments.
  - **Map by Full Name**—Select this option to map UNIX and Windows users who have identical full names.
3. The **Windows <-> UNIX Group Mapping Choice** section lets you determine the group mapping settings. Select one of the following:
  - **Default Mapping**—Select this option if there is no pre-defined mapping rule between Windows and UNIX groups. New groups will be assigned a newly-generated, unique ID by the system.
  - **Map by Group Name**—Select this option to map UNIX and Windows groups that have identical group names.
  - **Map to Primary Group**—Select this option to map to the NFS group in the primary group field in the configured `passwd` file.
4. Click **Apply** to save your changes.



# Adding a Map

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**.

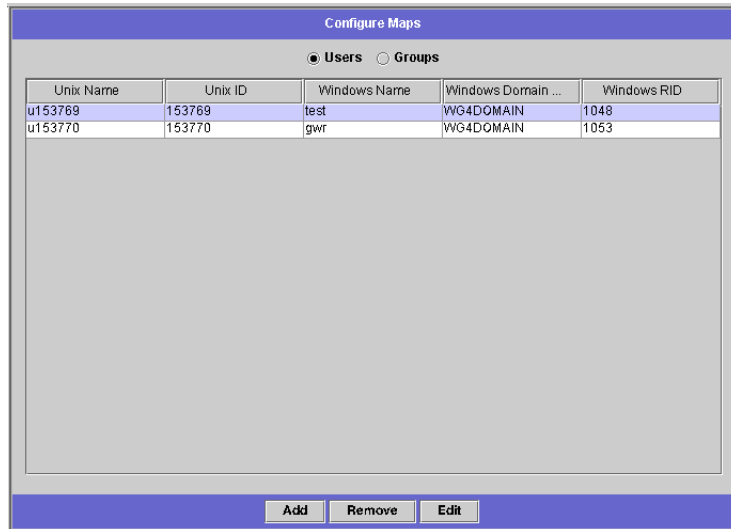


FIGURE 8-8 The Configure Maps Panel

2. Click **Add**.

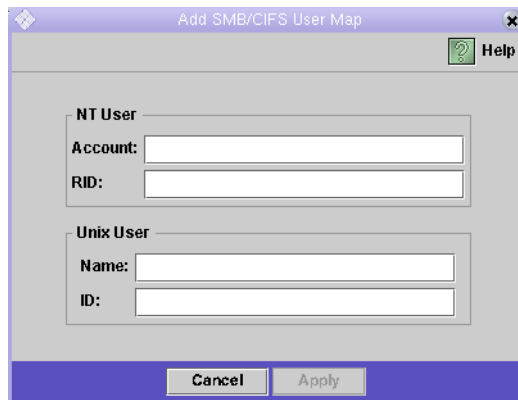


FIGURE 8-9 The Add SMB/CIFS User Map Dialog Box

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.

---

## Setting File Directory Security

### 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 Sun StorEdge 5310 NAS Appliance 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 111 for instructions on setting share-level security while adding a share. See "Editing Shares" on page 115 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 Sun StorEdge 5310 NAS Appliance server 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 StorEdge 5310 NAS Appliance supports security on files and directories only, and setting security on a share will pass that security assignment to the underlying directory.

---

To set security:

1. Open Windows Explorer.
2. Click Tools > Map Network Drive.

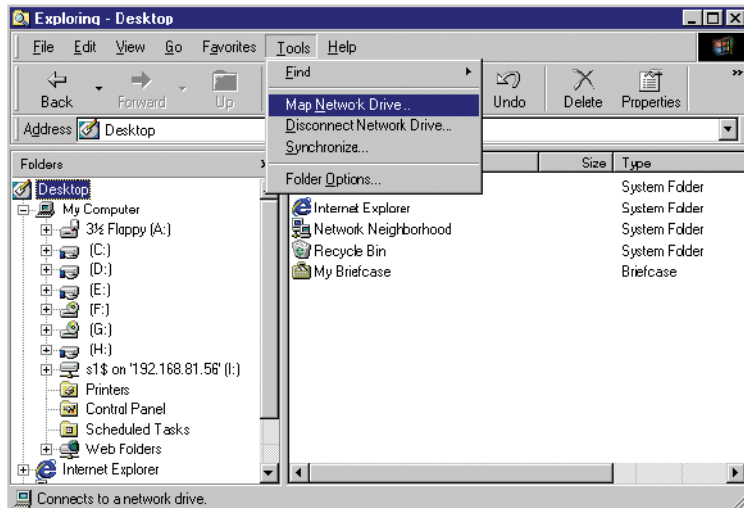


FIGURE 8-10 Mapping a Network Drive

3. In the Map Network Drive dialog box, select a drive letter from the Drive drop-down list box.

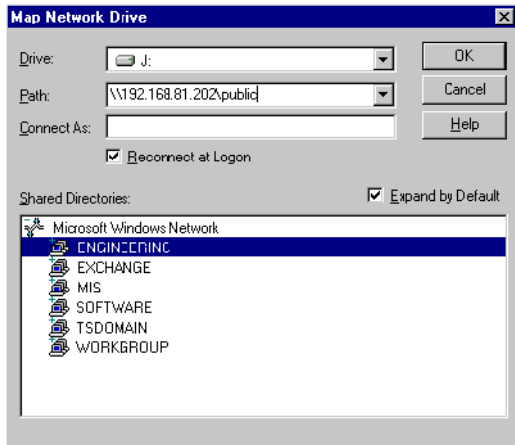


FIGURE 8-11 The Map Network Drive Dialog Box

4. Locate and select the Sun StorEdge 5310 NAS Appliance server.
5. Click OK.
6. From the Windows Explorer window, right-click on the Sun StorEdge 5310 NAS Appliance server share for which you want to define user-level permissions.
7. Select Properties from the drop-down list.
8. Select the Security tab in the Properties dialog box.

9. Click the Permissions button.

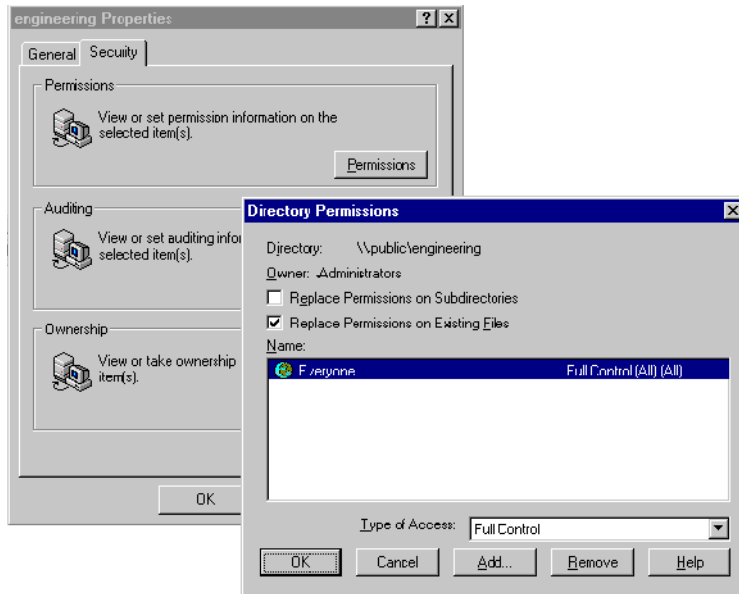


FIGURE 8-12 The Directory Permissions Dialog Box

10. Set the desired permissions. (See your Windows documentation for more information on setting permissions.)
11. Click OK.



## Shares, Quotas, and Exports

---

This chapter describes the various methods of controlling user access to the files and volumes on the Sun StorEdge 5310 NAS Appliance system.

---

### 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 StorEdge 5310 NAS Appliance.

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.

### About Static Shares

A shared resource, or **share**, is a local resource on a server that is accessible to Windows clients on the network. On a NAS server, 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. A static share is created to allow that user to map their home directory as a network drive 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 follows:

**TABLE 9-1** Share Path Examples

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

If defining and maintaining a static home directory share for each Windows user that has access to the system is inconvenient, you can use the autohome feature. Autohome shares are temporary shares created when a user logs on to the system and removed when the user logs off. See "About Autohome Shares" on page 117 for more information.

## Configuring Static Shares

The **Configure Shares** panel allows you to add, view, and update static SMB shares.

The table at the top of the **Configure Shares** panel shows information about all existing SMB shares in the Sun StorEdge 5310 NAS Appliance. 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.

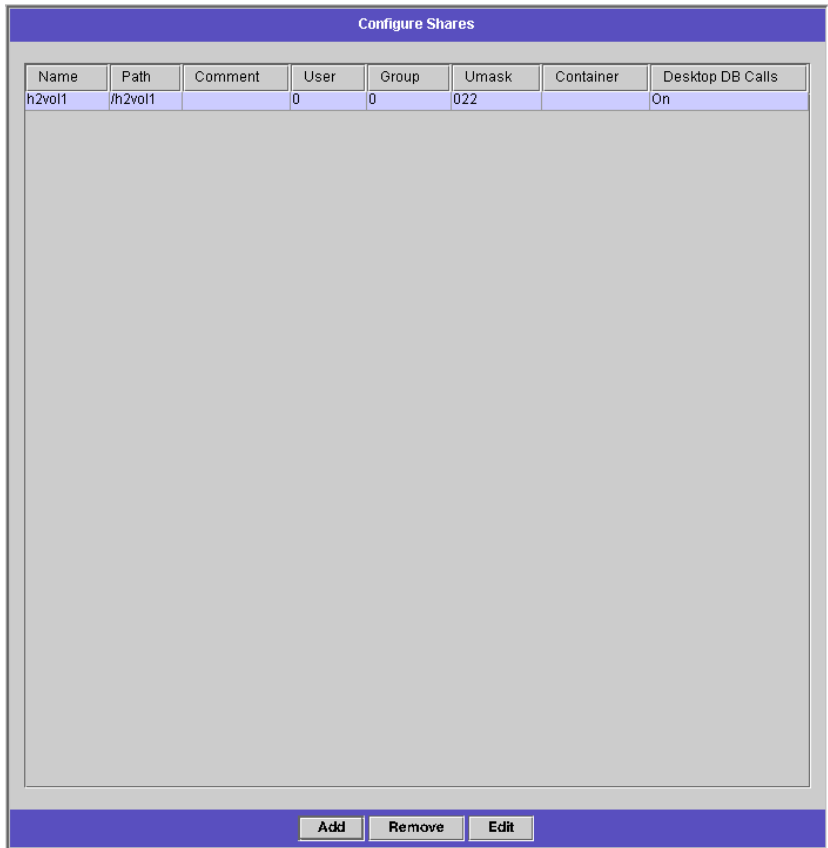


## Creating Static Shares

You must create a file volume before you can create a share. For more information, see "Creating a File Volume or a Segment" on page 50.

To add a new SMB share:

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



**FIGURE 9-1** The Configure Shares Panel

## 2. Click Add.

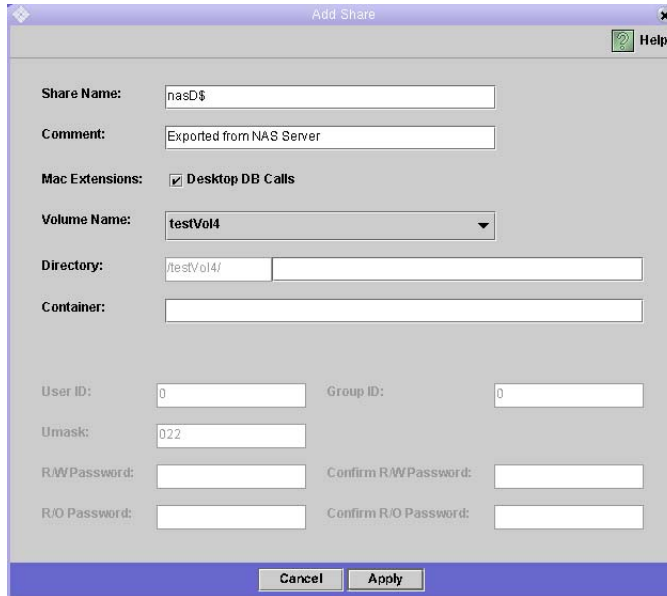


FIGURE 9-2 The Add Share Dialog Box

3. Type the name of the share you want to add in the Share Name field. This is the name that users see on the network. The name cannot be longer than fifteen characters. The following characters are invalid:  
= | : ; \ " ? < > \* /
4. Optionally, add a Comment to describe the share. You can enter up to 60 alphanumeric characters.
5. Select the Desktop DB Calls checkbox in the Mac Ext. section to allow the Sun StorEdge 5310 NAS Appliance to 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 StorEdge 5310 NAS Appliance.
6. Select the volume to share from the list of available volumes in the Volume Name drop-down list.
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. **The Container field (optional) specifies the ADS container in which to publish the share. If you enabled ADS in the Set Up ADS panel, this field is available. However, even if ADS is enabled you are not required to specify an ADS container. To specify the container, enter the ADS path location for the share in LDAP DN notation. See "Publishing Shares in ADS" on page 86 for more information.**
9. **The User ID, Group ID, and Password fields are only available if you enabled Windows Workgroup mode (not NT Domain mode) on the Sun StorEdge 5310 NAS Appliance. Refer to "Configuring Windows Security" on page 31 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 StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance 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 "Managing Quotas" on page 119.



---

**Caution – User ID**—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 comprised 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.

**TABLE 9-2** Umask Permission Examples

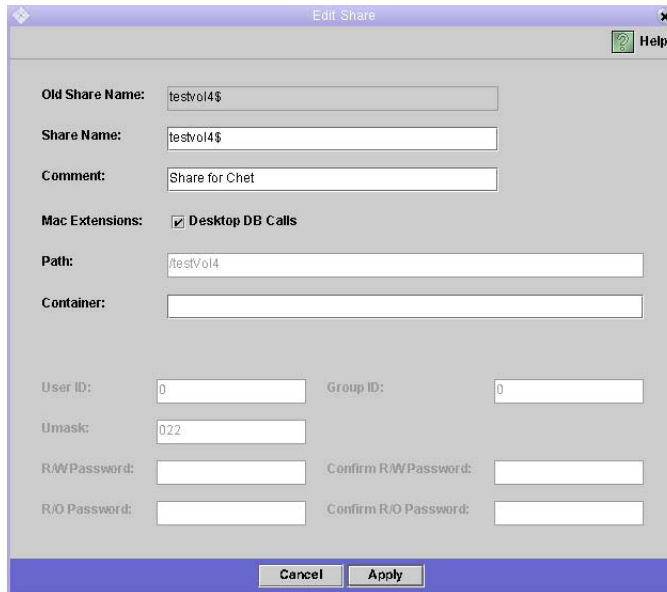
Umask	New Directory Permissions		New File Permissions	
	DOS R/W	DOS R/O	DOS R/W	DOS R/O
000	777 (rwxrwxrwx)	555 (r-xr-xr-x)	666 (rw-rw-rw)	444 (r--r--r--)
777	000 (-----)	000 (-----)	000 (-----)	000 (-----)
022	755 (rwxr-xr-x)	555 (r-xr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	555 (r-xr-xr-x)	664 (rw-rw-r--)	444 (r--r--r--)

11. Click **Apply** to save your changes.

## Editing Shares

To update the attributes of an existing SMB share:

1. In the navigation panel, select **Windows Configuration > Configure Shares**.
2. Select the share you want to update.
3. Click **Edit**.



**FIGURE 9-3** The Edit Share Dialog Box

4. The **Old Share Name** field displays the current name of the share. If you want to change it, enter the new name in the **Share Name** field. The following characters are invalid for the share name:  
= | : ; \ " ? < > \* /
5. You can 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 Sun StorEdge 5310 NAS Appliance 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 StorEdge 5310 NAS Appliance.
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 ADS container in which the share is published. This field is available only if you have enabled ADS for the Sun StorEdge 5310 NAS Appliance in the Set Up ADS panel. Enter the ADS path location for the share in LDAP DN notation. See "Setting Up ADS" on page 81 for more information.
9. The User ID, Group ID, and Password fields are only available if you enable Windows Workgroup mode (not NT Domain mode) on the Sun StorEdge 5310 NAS Appliance. Refer to "Configuring Windows Security" on page 31 for information on enabling Windows security models. See step 9. on page 113 for detailed information on these fields.
10. You can change the Umask setting using the rules specified for the Umask field under "Creating Static Shares" in step 10. on page 114.
11. Click Apply to save your changes.

## Removing Shares

To remove an SMB/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 **Yes** to remove the share.

## Configuring SMB/CIFS Clients

After you have configured the security and network settings, the Sun StorEdge 5310 NAS Appliance becomes visible to SMB/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 StorEdge 5310 NAS Appliance icon in the **Network Neighborhood** window.

If they map the network drive, they need the Universal Naming Convention (UNC) path for the Sun StorEdge 5310 NAS Appliance, 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 StorEdge 5310 NAS Appliance on the network.

## Windows 2000, XP, and 2003

If ADS is not installed, users connect either by mapping the network drive from Windows Explorer, or by clicking the Sun StorEdge 5310 NAS Appliance icon in the **My Network Places** window.

If they map the network drive, they need the UNC path for the Sun StorEdge 5310 NAS Appliance, 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 StorEdge 5310 NAS Appliance on the network.

If ADS is installed, users can connect to the Sun StorEdge 5310 NAS Appliance by clicking on a Sun StorEdge 5310 NAS Appliance 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 StorEdge 5310 NAS Appliance, which consists of a computer name and share name as follows: `\\computer_name\share_name`.

## About Autohome Shares

The SMB/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 may automatically log a user off after fifteen 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 Sun StorEdge 5310 NAS Appliance (for example, in an Explorer window), the share automatically reappears.

---

**Note** – All autohome shares are removed when the system reboots.

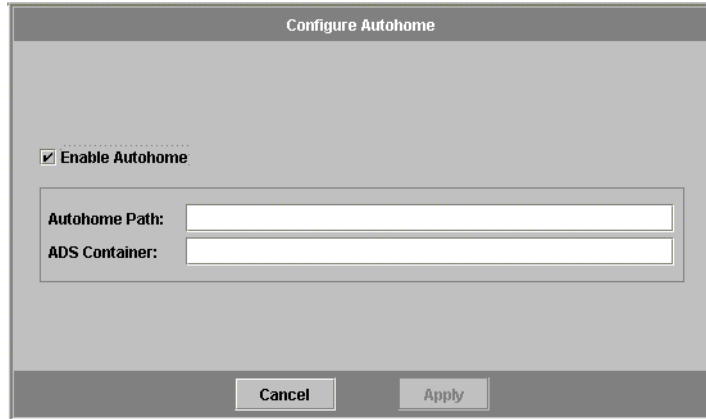
---

## Configuring Autohome Shares

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

To enable autohome shares on the Sun StorEdge 5310 NAS Appliance:

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



**FIGURE 9-4** The Configure Autohome Panel

2. Select the **Enable Autohome** checkbox.
3. Enter the **Autohome Path**. For more information on the path, see "About Autohome Shares" on page 117.



4. Enter the ADS Container. For more information, see "Active Directory Services" on page 80.
5. Click Apply to save your changes.

---

## Managing Quotas

The **Manage Quotas** panels let you administer quotas on Sun StorEdge 5310 NAS Appliance 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 "Adding a User or Group Quota Setting" on page 120 to set space and file limits for users and groups. Refer to "Configuring Directory Tree Quotas" on page 124 to set space and file limits for specific Sun StorEdge 5310 NAS Appliance directories.

## 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 **root user** and **root group** are automatically set to have no hard or soft limits for space or files. The settings for the **default user** and **default group** are the settings used for all users and groups that do not have individual quotas.

## About Hard and Soft Limits

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 TB. For the number of files, the hard limit can be no more than four billion files.

The **root user** and **root group** are automatically set to have no hard or soft limits for space or files.

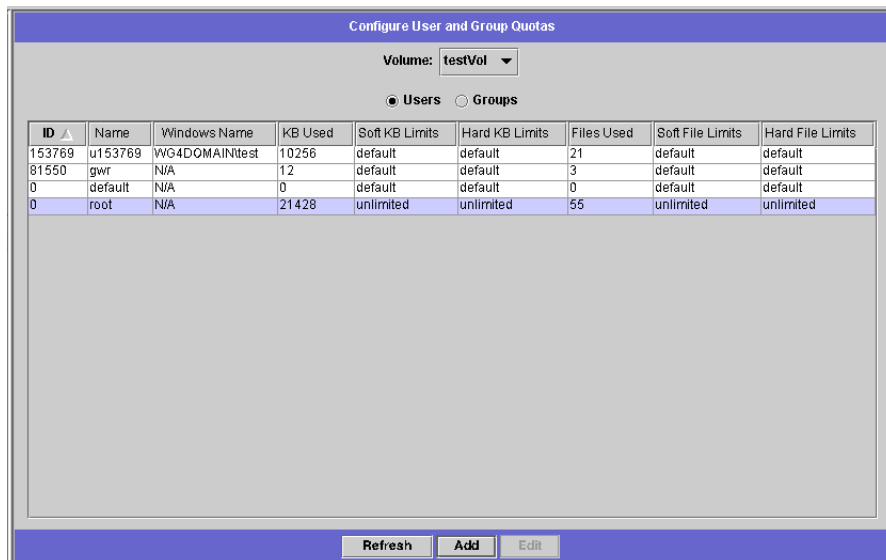
## Adding a User or Group Quota Setting

To enable quotas for the file volume:

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

To add a user or group quota:

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



**FIGURE 9-5** The Configure User and Group Quotas Panel

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.

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



FIGURE 9-6 The Add Quota Setting Dialog Box

- Select whether the designated user or group belongs to a UNIX or NT environment by clicking on the appropriate option button.
- Select the appropriate user or group name (and Domain name for NT users or groups).
- Set the disk space limits for the selected user or group. Choose among the following three options:
  - Default**—Choose this option to set the hard and soft limits to be the same as that of the default user or group.
  - No Limit**—Choose this option to allow unlimited space to the user or group.
  - Custom**—Choose this option to set a particular limit. Select whether the quota is displayed in **KB**, **MB**, or **GB**. Then enter the **Soft** and **Hard** space limits for the user or group.

---

**Note** – When defining user quotas you must set both hard and soft limits.

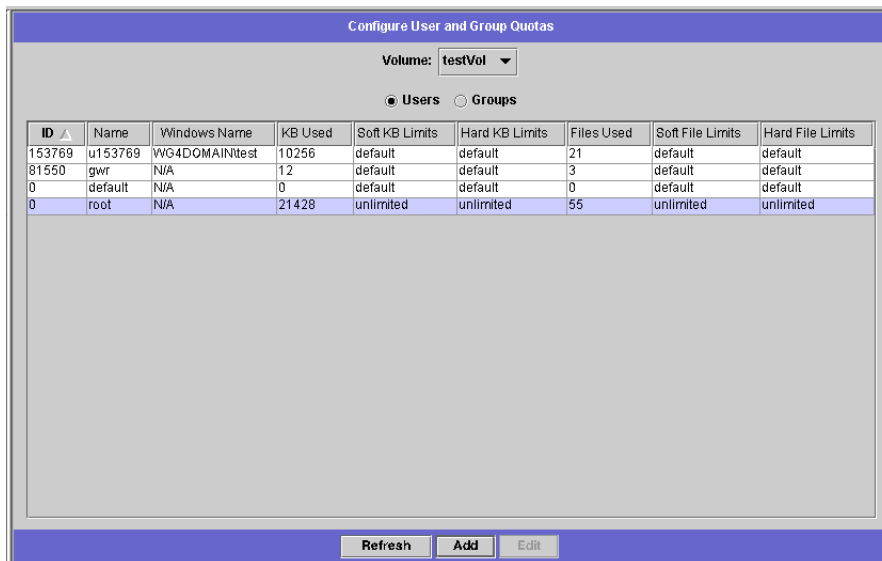
---

8. Set limits on the number of files a user or group can write to the file volume. Choose among the following three options:
  - **Default**—Choose this option to set the hard and soft limits to be the same as that of the default user or group.
  - **No Limit**—Choose this option to let the user or group write an unlimited number of files to the file volume.
  - **Custom**—Choose this option to set a particular file limit. Then enter the **Soft** and **Hard** limits for the number of files.
9. Click **Apply** to save your changes.

## Editing a User or Group Quota Setting

To edit a user or group quota:

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



**FIGURE 9-7** The Configure User and Group Quotas Panel

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.

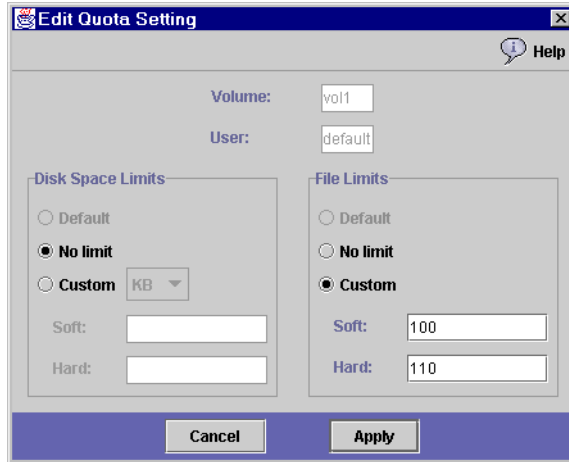


FIGURE 9-8 The Edit Quota Setting Dialog Box

5. Edit the disk space limits for the selected user or group. Choose among the following three options:
  - **Default**—Choose this option to set the hard and soft limits to be the same as that of the default user or group.
  - **No Limit**—Choose this option to allow unlimited space usage by the user or group.
  - **Custom**—Choose this option to set a particular limit. Select whether the quota is reported in **KB**, **MB**, or **GB**. Then enter the **Soft** and **Hard** space limits for the user or group.
6. Edit the limits on the number of files a user or group can write to the file volume. Choose between the following three options:
  - **Default**—Choose this option to set the hard and soft limits to be the same as those of the default user or group.
  - **No Limit**—Choose this option to let the user or group write an unlimited number of files to the file volume.
  - **Custom**—Choose this option to set a particular file limit. Then enter the **Soft** and **Hard** limits for the number of files.
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** dialog box, click the **Default** option in both the **Disk Space Limits** and **File Limits** sections.
5. Click **Apply** to remove the quota setting.

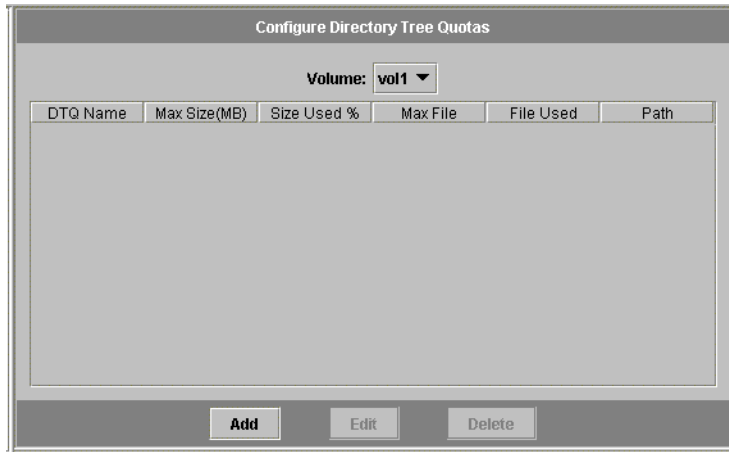
## Configuring Directory Tree Quotas

The **Configure Directory Tree Quotas (DTQ)** panel lets you administer quotas for specific directories in the Sun StorEdge 5310 NAS Appliance 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.

## Adding a Directory Tree Quota

To create a directory tree with a DTQ:

1. In the navigation panel, select **File Volume Operations > Manage Quotas > Configure Directory Tree Quotas**.



**FIGURE 9-9** The Configure Directory Tree Quotas Panel

2. Select the file volume for which you are configuring a directory tree quota from the drop-down list.

3. Click Add.

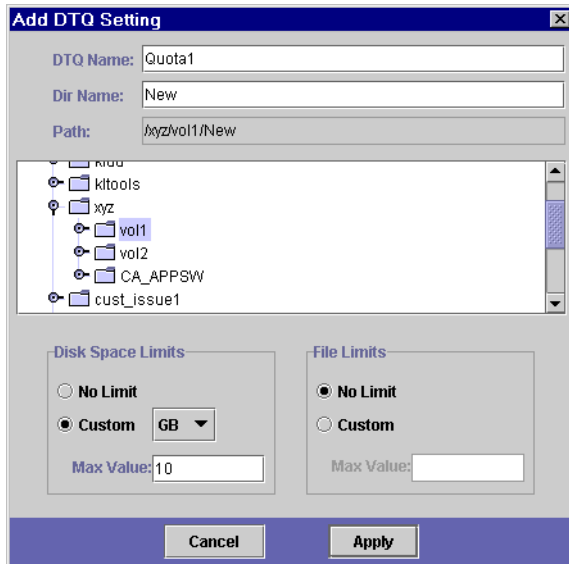




FIGURE 9-10 The Add DTQ Setting Dialog Box

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 to the  position, 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. Selecting No Limit allows 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 MB or GB and enter the disk space limit in the Max Value field. Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.



- In the File Limits field, select the maximum number of files that can be written to this directory, either No Limit or Custom. Selecting No Limit allows 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.
- Click Apply to add the quota.

## Editing a Directory Tree Quota

To edit an existing directory tree quota:

- In the navigation panel, select File Volume Operations > Manage Quotas > Configure Directory Tree Quotas.
- Select the quota you want to edit from the table, then click Edit.

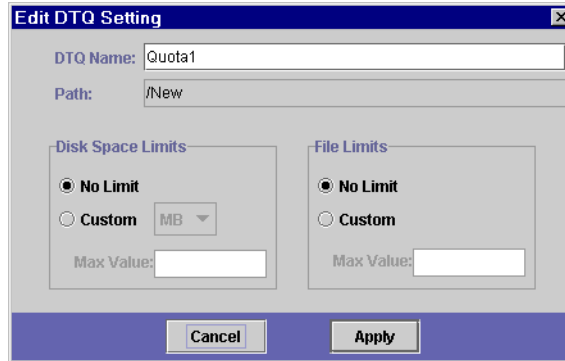


FIGURE 9-11 The Edit DTQ Setting Dialog Box

- 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.
- In the Disk Space Limits section, select the disk space limit for the directory; either No Limit or Custom. Selecting No Limit allows unlimited disk space usage for the directory. Select Custom to assign a maximum amount of disk space.
- Choose whether the quota is reported in MB or GB, and enter the disk space limit in the Max Value field. Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.
- In the File Limits section, select the maximum number of files to be written to this directory; either No Limit or Custom. Selecting No Limit lets you 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

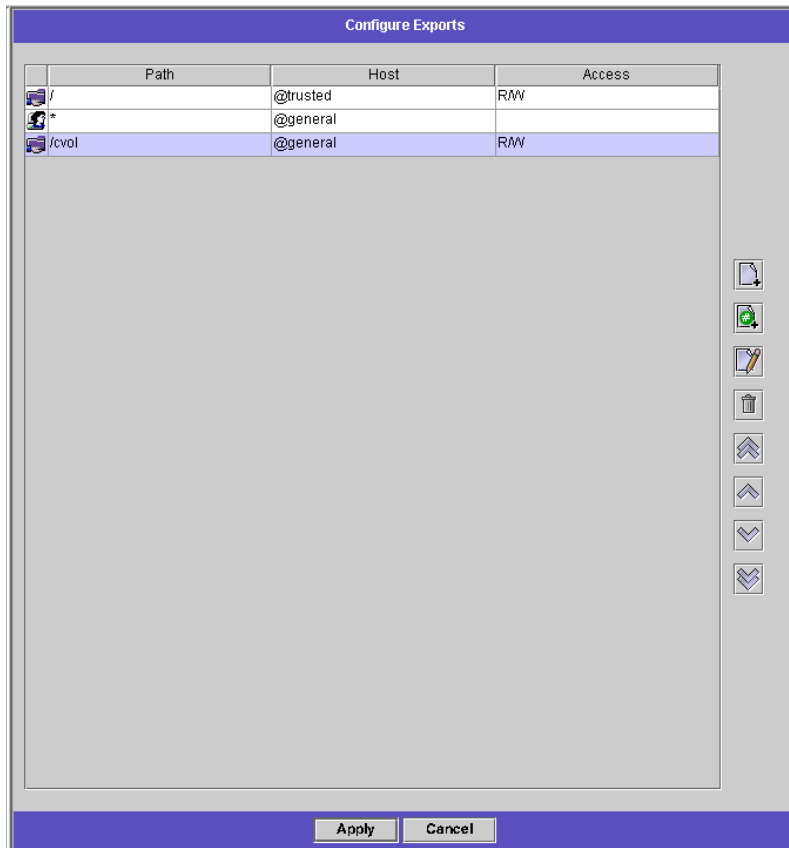
Network File System (NFS) exports let you specify access privileges for UNIX (and Linux) users. The table in the **Configuring Exports** panel shows the current NFS export information, including the accessible directories, host name, and access level (Read/Write or Read/Only) for each export.

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 "Configuring Hosts" on page 99 for information about trusted hosts.

# Creating Exports

To specify access privileges for a particular UNIX host:

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



**FIGURE 9-12** The Configure Exports Panel

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

2. Click  (Add button) to add an export.

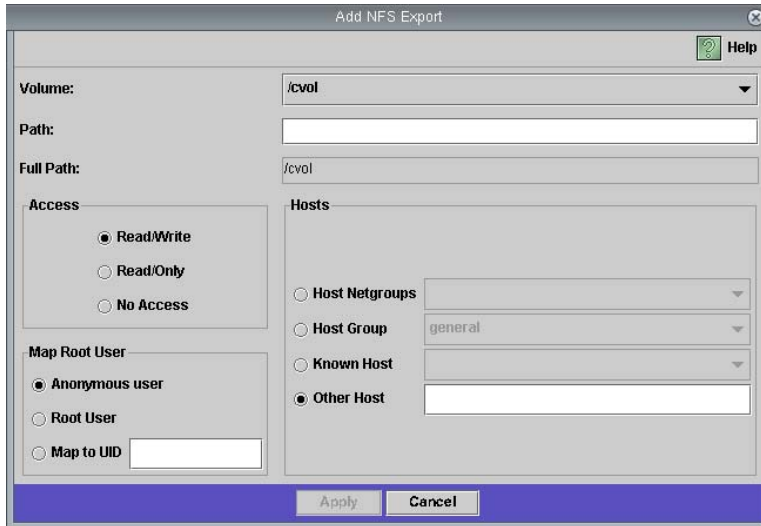



FIGURE 9-13 The Add NFS Export Dialog Box

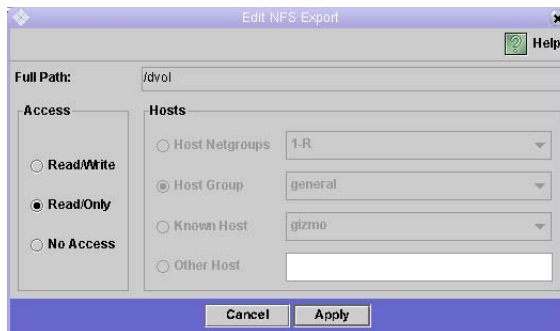
3. In the Volume box, select the volume for which you want to grant UNIX NFS host access.
4. In the Path box, specify the directory for which you want to grant UNIX NFS host access. Leaving this field blank exports the root directory of the volume.
5. In the Access section, specify whether the host(s) 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 an NFS export. Choose from the following:
  - **Host Netgroups**—To select a netgroup, select this option button. From the drop-down list, select the netgroup for which you are defining this export.
  - **Host Group**—To select a host group, select this option button. From the drop-down list, 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 drop-down list, 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 change the access rights for a particular volume:

1. In the navigation panel, select **UNIX Configuration > Configure NFS > Configure Exports**.
2. Select the export you want to change, and click  (Edit button).




**FIGURE 9-14** The Edit NFS Export Dialog Box

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 an NFS export, click on the export in the **Configure Exports** panel, and

click  (Remove button).

## Sun StorEdge 5310 NAS Appliance Options

---

This chapter provides instructions for activating options you can purchase for the Sun StorEdge 5310 NAS Appliance system. The following options are available and described in this chapter:

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

---

## Activating Sun StorEdge 5310 NAS Appliance Options

To activate Sun StorEdge 5310 NAS Appliance 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 an option:

1. In the navigation panel, select **System Operations > Activate Options** and click **Add** to add the license.

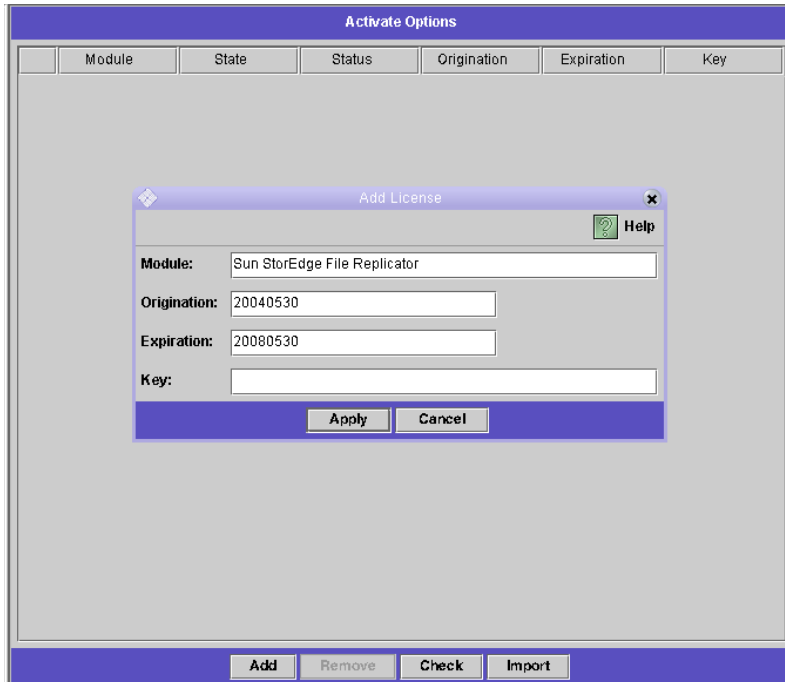


FIGURE 10-1 The Activate Options Panel

2. In the Add License dialog box enter the Module name provided by Sun (for example, Sun StorEdge 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.
5. Enter the license Key provided by Sun.
6. Click **Apply** to activate the option.

For Sun StorEdge File Replicator you must perform additional steps on the mirrored server. Refer to "Activating Sun StorEdge File Replicator" on page 139 for instructions.



7. If you have never set the time and date, the system will prompt you to do so.

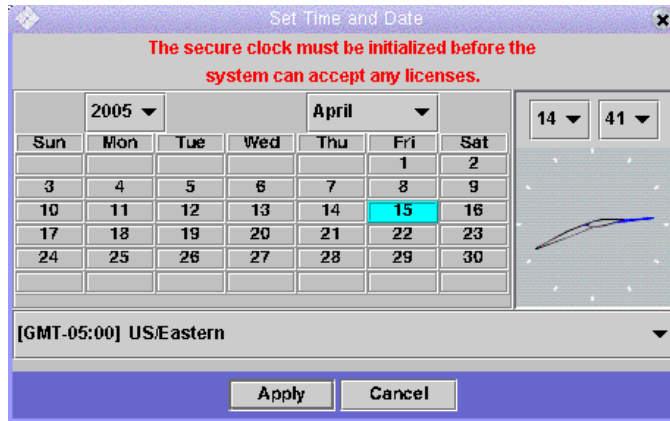


FIGURE 10-2 The Set Time and Date Panel

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. You will be prompted to confirm that the new time and date are accurate.

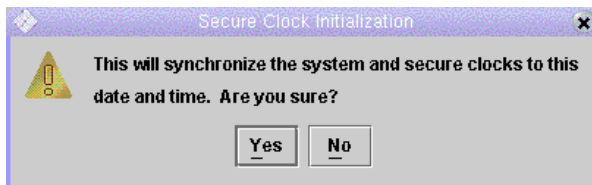


FIGURE 10-3 The Secure Clock Initialization Dialog

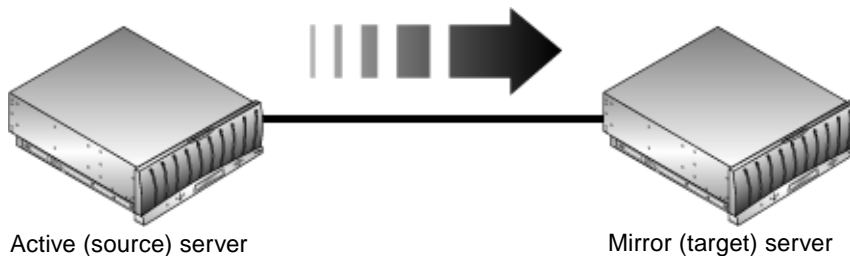
If the new time and date are correct, click **Yes**. If not, click **No** and set the time and date correctly.

---

# Sun StorEdge File Replicator

## About Sun StorEdge 5310 NAS Appliance Mirroring

Mirroring allows you to duplicate any or all of the file volumes of one Sun StorEdge NAS server onto another Sun StorEdge NAS server. The source server is called the *active server* and the target server is called the *mirror server*. The image below illustrates this relationship:



**FIGURE 10-4** The Mirror Relationship

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

The mirroring method used in the Sun StorEdge 5310 NAS Appliance 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.

## Before You Begin Mirroring

Before you begin, make sure you have the following:

- Two Sun StorEdge 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 100Mb Ethernet or 1000Mb Ethernet. The servers may be directly connected using a cross-over cable, or 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 1GB.

---

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

---

## Configuring Active and Mirror Systems

When setting up your systems, designate the roles of the ports connecting the mirroring servers to one another (see "Configuring the Dedicated Network Ports" on page 138). Then configure mirroring on the active and mirror systems using the Web Administrator interface (see "Configuring Mirrored File Volumes" on page 139). Configure each system independently.

## Configuring the Dedicated Network Ports

To configure the dedicated network ports:

1. In the navigation panel of the active server, select **Network Configuration > Configure TCP/IP > Configure Network Adapters**.



FIGURE 10-5 The Configure Network Adapters Panel

2. If you have not done so already, assign the 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 TCP/IP, see "Configuring the Network Ports" on page 27.

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 215.**
6. **Click Apply to save changes.**

## Configuring Mirrored File Volumes

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 GB can be mirrored. Once a file volume is mirrored, the original file volume cannot be renamed while the mirroring connection is maintained.

---

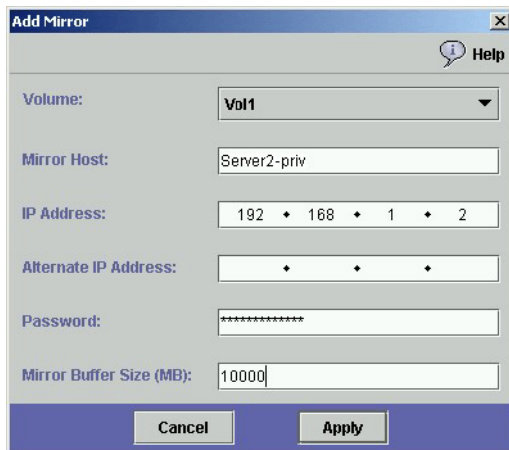
There can be no I/O activity to the file volume being mirrored from the active server during initial mirror synchronization.

## Activating Sun StorEdge File Replicator

After you have activated the Sun StorEdge File Replicator option (see "Activating Sun StorEdge 5310 NAS Appliance Options" on page 133), you must also activate the option on the remote server that contains file volumes you want to mirror.

1. **Log into Web Administrator on the server containing the file volume(s) you want to mirror.**

2. In the Add License dialog box enter the Module name provided by Sun (Sun StorEdge 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.
5. Enter the license Key provided by Sun.
6. Click Apply to activate Sun StorEdge File Replicator.
7. On the navigation panel select File Replicator > Manage Mirrors.
8. Click Add.



**FIGURE 10-6** The Add Mirror Dialog Box

9. Select the file volume to be mirrored from the Volume drop-down list. The file volume to be mirrored must be equal to or larger than 1 GB.
10. Enter a distinct name for the mirror server in the Mirror Host field.
11. Enter the IP Address of the mirror system. This should be the IP address chosen for the mirroring NIC on the mirror system.
12. Enter the Alternate IP Address, optional.

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

13. 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.

14. Enter the size (in MB) of the Mirror Buffer.

The mirror buffer stores file system write transactions while they are being transferred to the mirror server. The size of the mirror buffer depends on a variety of factors, but must be at least 100 MB. You may want to create a mirror buffer that is approximately 10% 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. The file volume free space on the active server is reduced by the allocation size of the mirror buffer.

15. Be sure there is no I/O activity to the source file volume on the active server while the mirror is being created. Click Apply to create the mirror.

The mirror creation process begins. When the mirror reaches an In Sync status in the Manage Mirrors panel (Figure 10-7), the mirrored file volume is mounted as read-only. I/O activity can resume once the mirror reaches In Sync status.

Volume	Active Server	Mirror Server	Status
v01	192.168.76.135 (local)	candy88-priv	In Sync 100%
v02	192.168.76.135 (local)	candy88-priv	In Sync 100%
v03	192.168.76.135 (local)	candy88-priv	In Sync 100%
v04	192.168.76.135 (local)	candy88-priv	In Sync 100%
v05	192.168.76.135 (local)	candy88-priv	In Sync 100%
v06	192.168.76.135 (local)	candy88-priv	In Sync 100%
v07	192.168.76.135 (local)	candy88-priv	In Sync 100%
v08	192.168.76.135 (local)	candy88-priv	In Sync 100%
v09	192.168.76.135 (local)	candy88-priv	In Sync 100%
v10	192.168.76.135 (local)	candy88-priv	In Sync 100%
v11	192.168.76.135 (local)	candy88-priv	In Sync 100%
v12	192.168.76.135 (local)	candy88-priv	In Sync 100%
v13	192.168.76.135 (local)	candy88-priv	In Sync 100%
v14	192.168.76.135 (local)	candy88-priv	In Sync 100%

FIGURE 10-7 The Manage Mirrors Panel

## Editing a Mirror

This section allows you to edit the alternate IP address(es) or mirror server administrator password of an existing 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.

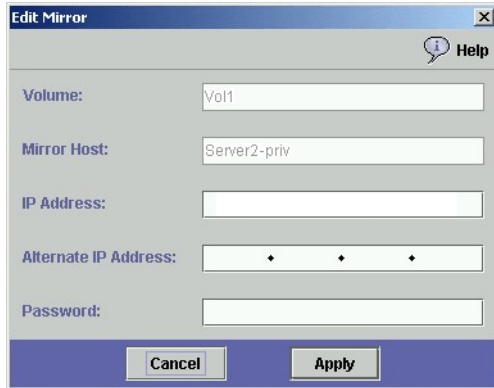


FIGURE 10-8 The Edit Mirror Dialog Box

4. Edit the 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.

## 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 re-established. 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 Sun StorEdge 5310 NAS Appliance automatically sends warnings through email notification, the system log file, SNMP traps, and the LCD panel when the mirror buffer is filled to certain threshold percentages.

To set up the threshold alert:

1. In the navigation panel, select **File Replicator > Set Threshold Alert**.

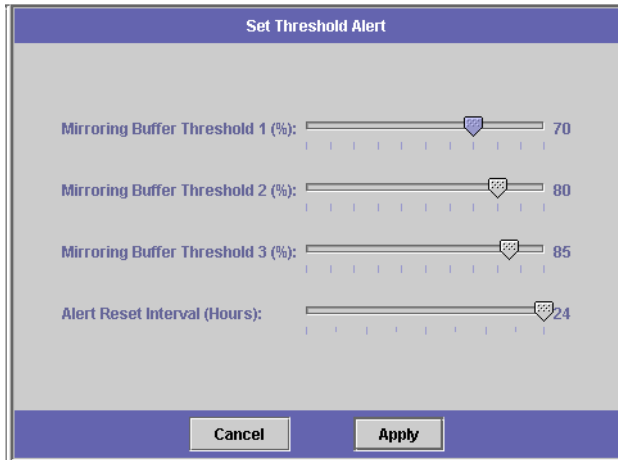


FIGURE 10-9 The Set Threshold Alert Panel

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%. This means that when the mirror buffer is 70% 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%.
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%.
5. Select the **Alert Reset Interval (Hours)**. This is the amount of time the Sun StorEdge 5310 NAS Appliance 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% and the **Alert Reset Interval** to two hours, the first alert is issued when the mirror buffer is 10% full. The Sun StorEdge 5310 NAS Appliance 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 (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:

1. In the navigation panel of the active server, select **File Replicator > Manage Mirrors**.

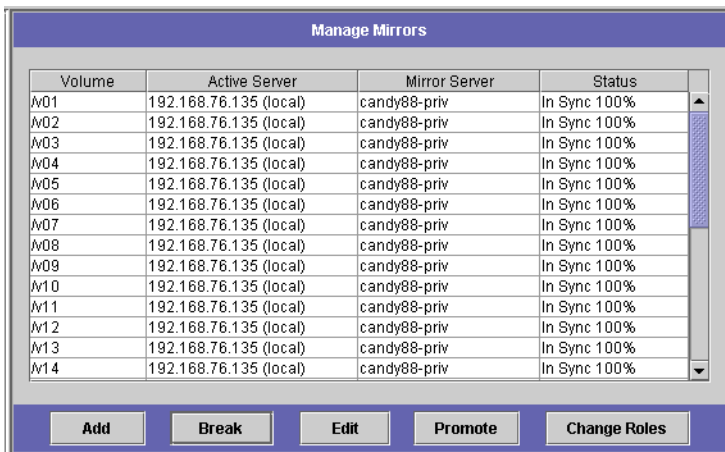


FIGURE 10-10 The Manage Mirrors Panel

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 145.

# Promoting a Mirrored File Volume

In the event that the active server fails, the mirror server provides fault tolerance 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 compliance-enabled volume cannot be promoted.

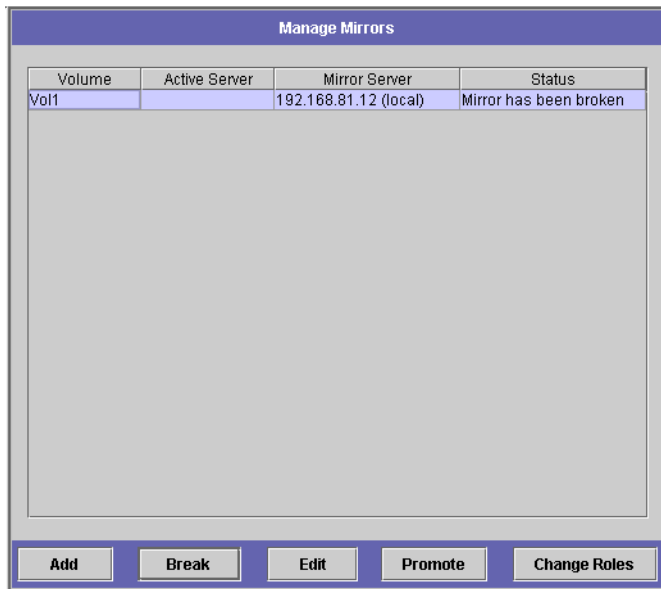
If you need temporary access to a compliance mirror volume, you can export it as a read-only file system without promoting it.

---

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 144 for instructions.

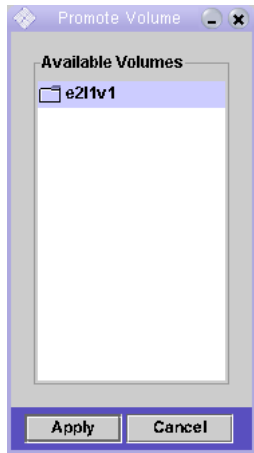
To promote a file volume on the mirror server:

1. In the navigation panel of the mirror server, select File Replicator > Manage Mirrors.



**FIGURE 10-11** The Manage Mirrors Panel

2. Click **Promote**.



**FIGURE 10-12** The Promote Volume Dialog Box

3. On the **Promote Volume** dialog box, 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. SMB share information is carried over automatically, but you must configure any NFS file volume access and NFS exports for this file volume again. For more information on setting up NFS exports, see "Setting Up NFS Exports" on page 128.

## Re-establishing a Mirror Connection

This procedure describes how to re-establish 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.

To re-establish a mirror connection:

- Make sure the mirror on *Server 1* is broken, see "Breaking the Mirror Connection on Server 1" on page 147.
- Delete the out-of-date file volume on *Server 1*, see "Deleting the Out-of-Date File Volume on Server 1" on page 148.
- Mirror the up-to-date file volume from *Server 2* back to *Server 1*, see "Mirroring the Up-to-Date Volume from Server 2 to Server 1" on page 149.
- Change role on Server 2, see "Changing Volume Roles" on page 150. At this point Server 1 would be active again and Server 2 would be the mirroring target.

## Breaking the Mirror Connection on *Server 1*

The connection between the active and mirror servers is illustrated below.



**FIGURE 10-13** The Mirror Relationship

When the active server is brought online, it may attempt to re-establish the mirror connection. Therefore you must break the mirror connection on the active server.

To break the mirror connection on the active server (if you did not already do so):

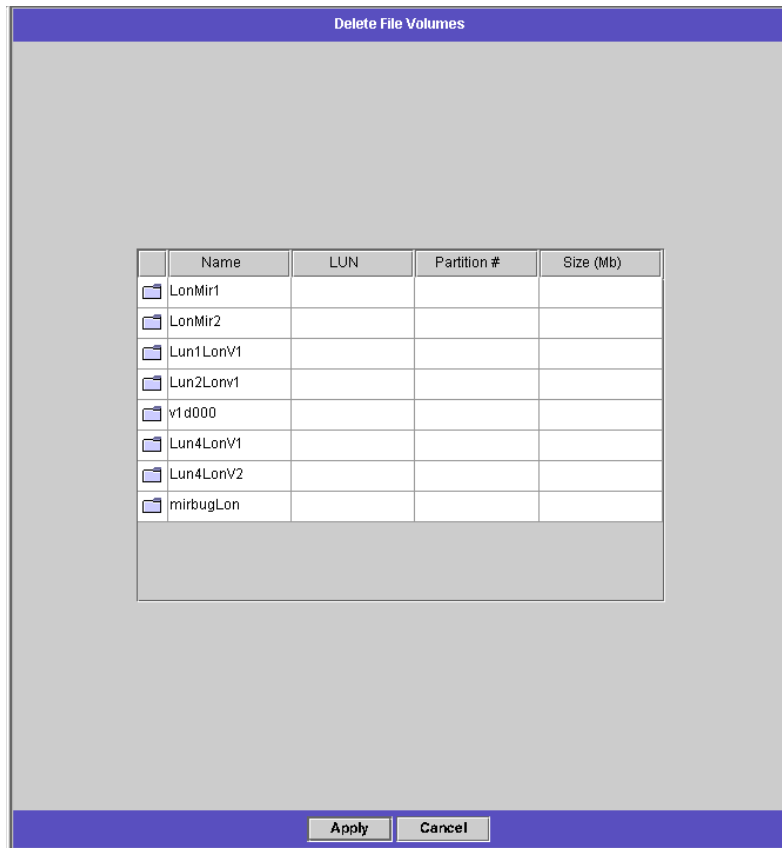
1. **Open a Web browser window to *Server 1*.**
2. **In the navigation panel, select File Replicator > Manage Mirrors.**

3. Select the mirror connection you want to break.
4. Click **Break**.

## Deleting the Out-of-Date File Volume on *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**.



**FIGURE 10-14** The Delete File Volumes Panel

2. Select the file volume that was being mirrored. Since 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 Volume from *Server 2* to *Server 1*

This section describes how to mirror the up-to-date file volume on the former mirror server (*Server 2*) back to the former active server (*Server 1*).

To mirror the 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**.

The screenshot shows a dialog box titled "Add Mirror". It has a "Help" icon in the top right corner. The fields are as follows:

- Volume:** A dropdown menu with "Vol1" selected.
- Mirror Host:** A text input field containing "Server1-priv".
- IP Address:** A text input field containing "192 + 168 + 1 + 1".
- Alternate IP Address:** A text input field containing three dots.
- Password:** A text input field containing eight asterisks.
- Mirror Buffer Size (MB):** A text input field containing "10000".

At the bottom of the dialog are two buttons: "Cancel" and "Apply".

**FIGURE 10-15** The Add Mirror Dialog Box

4. Select the file volume to be mirrored from the **Volume** drop-down list.
5. Enter the mirroring name of *Server 1* in the **Mirror Host** field.
6. Enter the **IP Address** of the *Server 1* port used for the mirroring connection.
7. Enter 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. **Enter the size of the Mirror Buffer. For more information about the mirror buffer, see "About Sun StorEdge 5310 NAS Appliance Mirroring" on page 136.**

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 150 for more information.**

You have re-established the original mirroring connection.

## Changing Volume Roles

An administrator can switch roles between an active volume and the mirror volume. Changing volume roles allows 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% in sync to change roles.

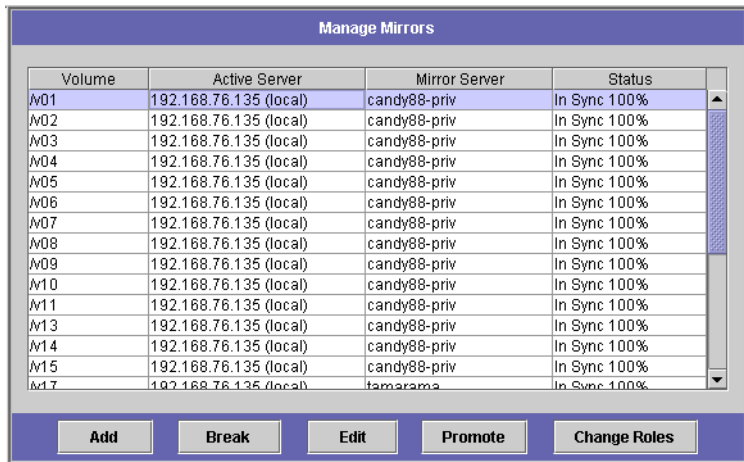
---

Changing roles can be initiated in the Manage Mirror panel from the active or mirror server.

To change roles:



1. In the navigation panel click File Replicator > Manage Mirrors.



The screenshot shows a window titled "Manage Mirrors" with a table containing the following data:

Volume	Active Server	Mirror Server	Status
v01	192.168.76.135 (local)	candy88-priv	In Sync 100%
v02	192.168.76.135 (local)	candy88-priv	In Sync 100%
v03	192.168.76.135 (local)	candy88-priv	In Sync 100%
v04	192.168.76.135 (local)	candy88-priv	In Sync 100%
v05	192.168.76.135 (local)	candy88-priv	In Sync 100%
v06	192.168.76.135 (local)	candy88-priv	In Sync 100%
v07	192.168.76.135 (local)	candy88-priv	In Sync 100%
v08	192.168.76.135 (local)	candy88-priv	In Sync 100%
v09	192.168.76.135 (local)	candy88-priv	In Sync 100%
v10	192.168.76.135 (local)	candy88-priv	In Sync 100%
v11	192.168.76.135 (local)	candy88-priv	In Sync 100%
v13	192.168.76.135 (local)	candy88-priv	In Sync 100%
v14	192.168.76.135 (local)	candy88-priv	In Sync 100%
v15	192.168.76.135 (local)	candy88-priv	In Sync 100%
v17	192.168.76.135 (local)	tamarama	In Sync 100%

Below the table are five buttons: Add, Break, Edit, Promote, and Change Roles.

FIGURE 10-16 The Manage Mirrors Panel

2. Select a volume in the Volume column.
3. Click Change Roles.

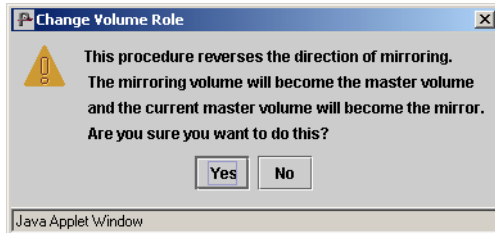


FIGURE 10-17 The Change Volume Role Dialog Box

4. Click Yes to confirm.

---

# 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.

---

**Note** – Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorEdge 5310 NAS Appliance system hardware. In particular, the Sun StorEdge 5300 RAID EU controller 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 EU 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 StorEdge 5310 NAS Appliance system. 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 "Create a File Volume or Segment Using the Create File Volume Panel" on page 51 to create a compliance-enabled volume.



---

**Caution** – Once you enable compliance archiving on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled.

---

For a technical overview of the features and programming interface for the Compliance Archiving Software, see "Compliance Archiving Software API" on page 269.

To change compliance archiving settings, see "Configuring the Compliance Archiving Software" on page 261.



# Monitoring

---

This chapter describes the monitoring functions of the Sun StorEdge 5310 NAS Appliance 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.

---

## Monitoring Functions

### Configuring SNMP

The **Configure SNMP** panel lets you enable or disable SNMP (Simple Network Management Protocol) communications, which let you conduct SNMP monitoring. The Sun StorEdge 5310 NAS Appliance supports SNMP monitoring only (not SNMP management).

To interpret Sun StorEdge 5310 NAS Appliance Message Information Blocks (MIB), you must copy the MIB files from <http://sunsolve.sun.com> to your network management system. Refer to your network management application documentation for information about how to use these files.


To set up SNMP:

1. In the navigation panel, select **Monitoring and Notification > Configure SNMP**.

Destination IP Address	Port #	Version	Community	Enable
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>

FIGURE 11-1 The Configure SNMP Panel

2. Select the **Enable SNMP** checkbox to enable SNMP.
3. Enter the SNMP community to which the Sun StorEdge 5310 NAS Appliance belongs in the **Server SNMP Community** field.
4. The **Contact Info** and **System Location** fields are description fields. In the **Contact Info** field, enter the name of the person who is responsible for this Sun StorEdge 5310 NAS Appliance 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 unused line 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 number**—Enter the port to which the Sun StorEdge 5310 NAS Appliance sends traps. The default value is port **162**.
  - **Version**—Choose the SNMP protocol version (either 1 or 2) from the drop-down list.
  - **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 .
8. Click Apply to save your changes.

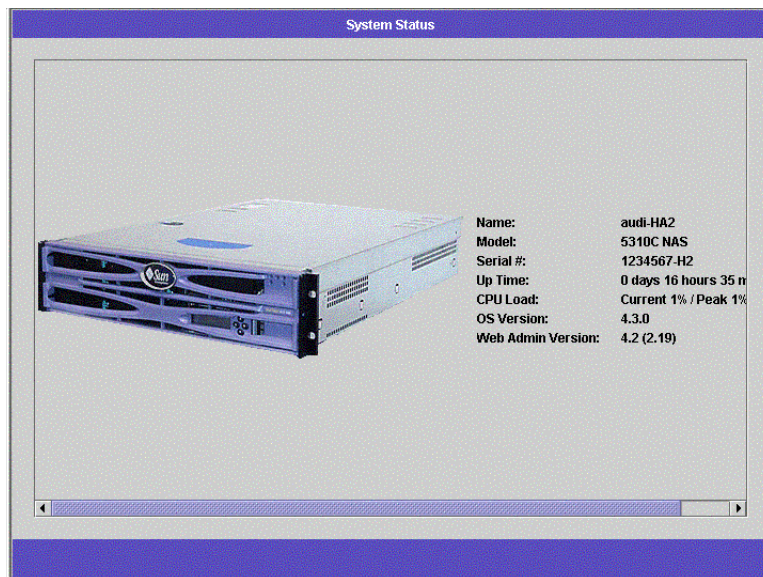
---

## Viewing Sun StorEdge 5310 NAS Appliance Status

Web Administrator 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.

When you first log in to Web Administrator, the Sun StorEdge 5310 NAS Appliance **System Status** panel displays the model and operating system information.




**FIGURE 11-2** The System Status Panel

This screen provides a read-only display of the following data:

- **Name**—The Sun StorEdge 5310 NAS Appliance server name
- **Model**—The Sun StorEdge 5310 NAS Appliance server model

- **Serial #**—The unique serial number of the Sun StorEdge 5310 NAS Appliance server
- **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

To return to this screen at any time, click the  button in the toolbar.

---

## 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. When it first starts up, the Sun StorEdge 5310 NAS Appliance creates a temporary log file in volatile memory to retain any errors that might occur during initial startup.

---

## Displaying the System Log

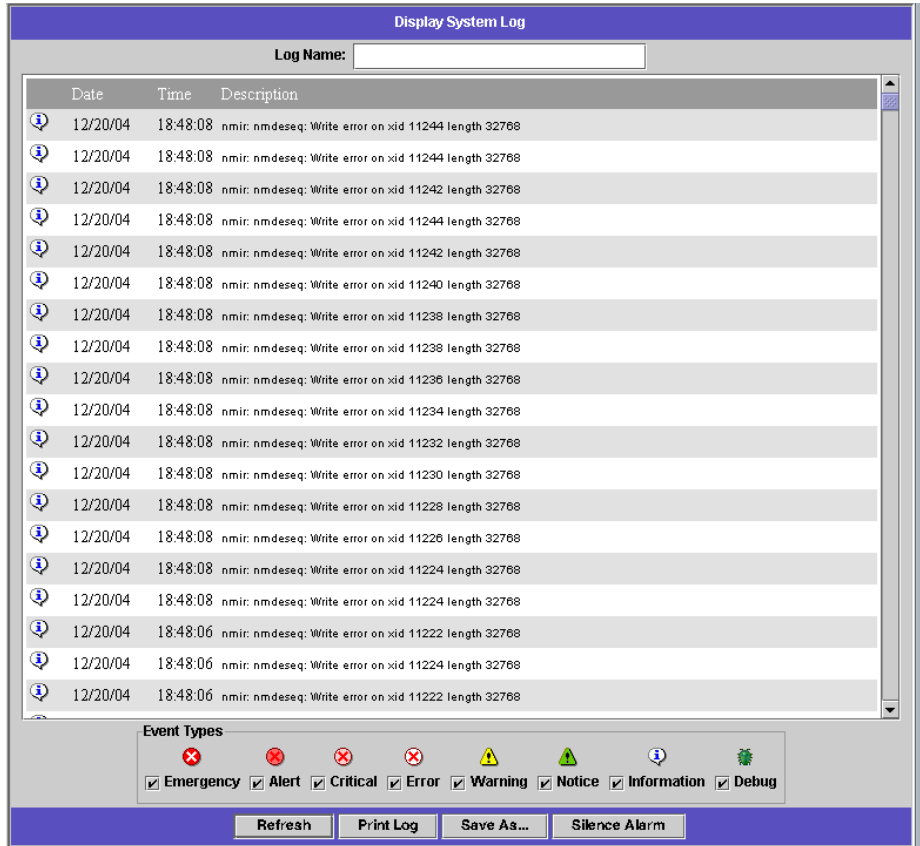
The **Display System Log** panel displays all system events, warnings, and errors, including the date and time they occurred. This panel automatically displays the most recent system events. Use the scroll bar to view earlier events.



---

**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.

---



**FIGURE 11-3** The Display System Log Panel

To view the 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 "System Events" on page 160 for more information.)
3. Click **Refresh**.

# System Events

The system log (see "Displaying the System Log" on page 158) logs eight (8) types of system events. Each event is represented by an icon.

TABLE 11-1 System Event Icons

---

	<b>Emergency</b> —Specifies emergency messages. These messages are not distributed to all users. Emergency priority messages are logged into a separate file for reviewing.
	<b>Alert</b> —Specifies important messages that require immediate attention. These messages are distributed to all users.
	<b>Critical</b> —Specifies critical messages not classified as errors, such as hardware problems. Critical and higher-priority messages are sent to the system console.
	<b>Error</b> —Specifies any messages that represent error conditions, such as an unsuccessful disk write.
	<b>Warning</b> —Specifies any messages for abnormal, but recoverable, conditions.
	<b>Notice</b> —Specifies important informational messages. Messages without a priority designation are mapped into this priority message.
	<b>Information</b> —Specifies informational messages. These messages are useful in analyzing the system.
	<b>Debug</b> —Specifies debugging messages.

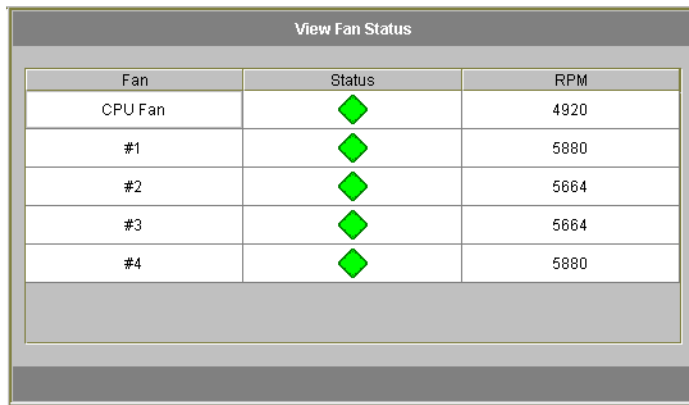
---

---

# Environmental Status

## Viewing Fan Status

To view the operational status and Revolutions Per Minute (RPM) of all fans in the Sun StorEdge 5310 NAS Appliance head unit, in the navigation panel, select **Monitoring and Notification > View Environmental Status > View Fan Status**.



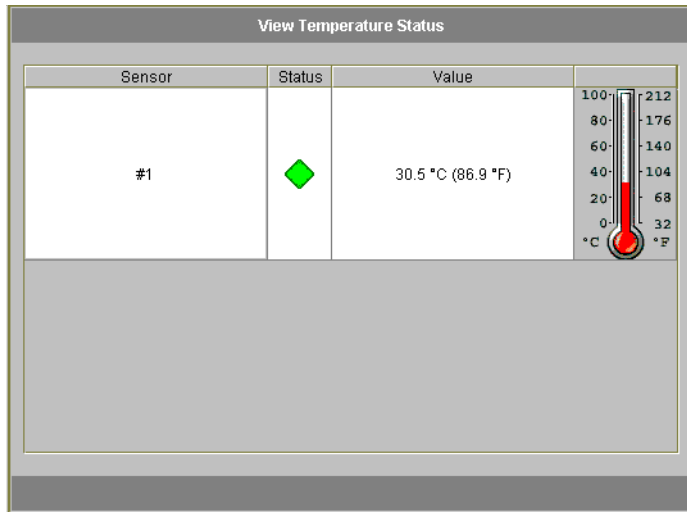
Fan	Status	RPM
CPU Fan	◆	4920
#1	◆	5880
#2	◆	5664
#3	◆	5664
#4	◆	5880

**FIGURE 11-4** The View Fan Status Panel

The table shows the current status of each fan. A green diamond in the **Status** column indicates that the fan RPM are normal. A red diamond indicates that the RPM have exceeded the acceptable range. If the RPM of any fan falls 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 Notification" on page 41.

# Viewing Temperature Status

To view temperature status in the Sun StorEdge 5310 NAS Appliance, in the navigation panel, select **Monitoring and Notification > View Environmental Status > View Temperature Status**.



**FIGURE 11-5** The View Temperature Status Panel

This screen displays the temperature of the sensors in the head unit. A green diamond in the **Status** column indicates that the Sun StorEdge 5310 NAS Appliance 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.

---

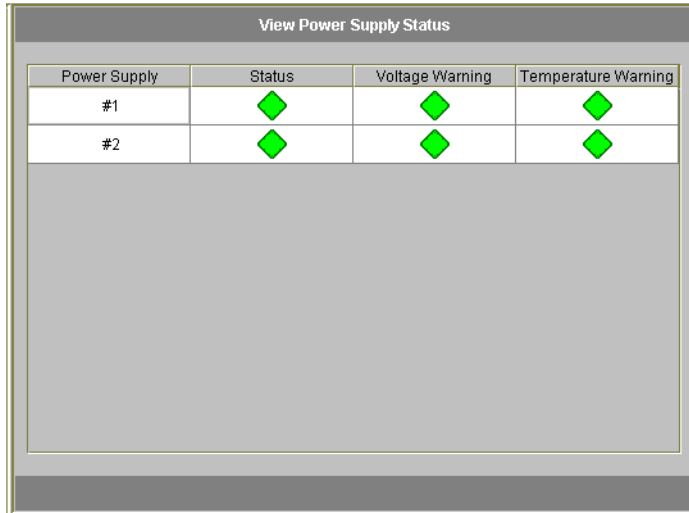
**Note** – You cannot change the temperature thresholds.

---

# Viewing Power Supply Status

The **View Power Supply Status** panel displays the current status of all Sun StorEdge 5310 NAS Appliance power supplies.

To display power supply status for the Sun StorEdge 5310 NAS Appliance, in the navigation panel, select **Monitoring and Notification > View Environmental Status > View Power Supply Status**.



Power Supply	Status	Voltage Warning	Temperature Warning
#1	◆	◆	◆
#2	◆	◆	◆

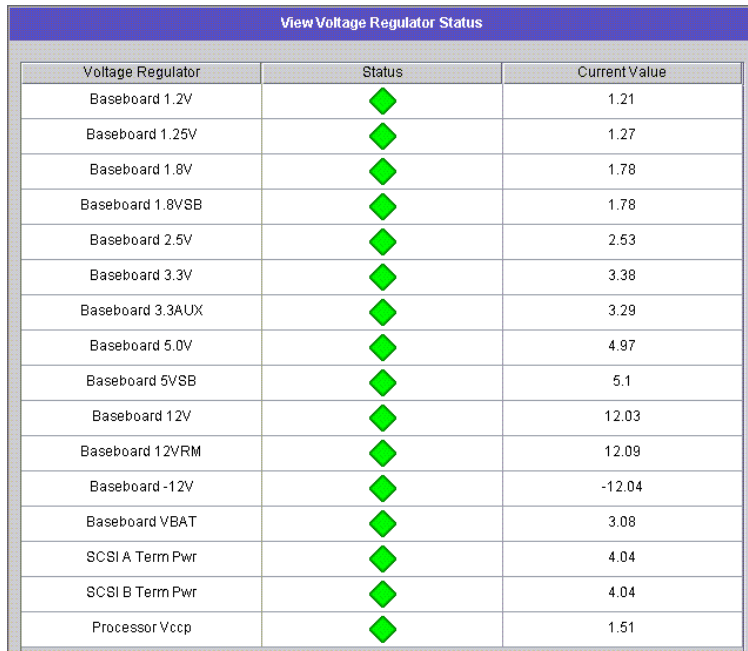
**FIGURE 11-6** The View Power Supply Status Panel

There are 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 Notification" on page 41.

# Viewing Voltage Status

To display the current voltage readings in the Sun StorEdge 5310 NAS Appliance, in the navigation panel, select **Monitoring and Notification > View Environmental Status > View Voltage Regulator Status**.



Voltage Regulator	Status	Current Value
Baseboard 1.2V	◆	1.21
Baseboard 1.25V	◆	1.27
Baseboard 1.8V	◆	1.78
Baseboard 1.8VSB	◆	1.78
Baseboard 2.5V	◆	2.53
Baseboard 3.3V	◆	3.38
Baseboard 3.3AUX	◆	3.29
Baseboard 5.0V	◆	4.97
Baseboard 5VSB	◆	5.1
Baseboard 12V	◆	12.03
Baseboard 12VRM	◆	12.09
Baseboard -12V	◆	-12.04
Baseboard VBAT	◆	3.08
SCSI A Term Pwr	◆	4.04
SCSI B Term Pwr	◆	4.04
Processor Vccp	◆	1.51

**FIGURE 11-7** The View Voltage Regulator Status Panel

See Table 11-2 for the acceptable range for each voltage.

**TABLE 11-2** Acceptable Voltage Ranges

<b>Voltage Value</b>	<b>Acceptable Range</b>
Baseboard 1.2V	1.133V to 1.250V
Baseboard 1.25V	1.074V to 1.406V
Baseboard 1.8V	1.700V to 1.875V
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

---

## Usage Information

### Viewing File Volume Usage

To view the used and free space of file volumes in the Sun StorEdge 5310 NAS Appliance, select **Monitoring and Notification** in the navigation panel. Then select **View File Volume Usage** to display file volume capacity and usage.

If usage of a file volume exceeds 95%, an email is sent to designated recipients.

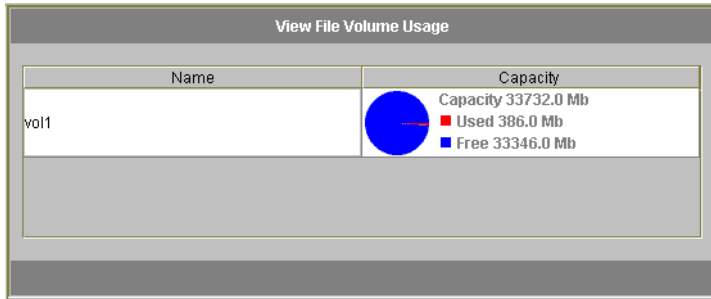


FIGURE 11-8 The View File Volume Usage Panel

## Viewing Statistics

### Viewing Network Activity

To display the number of I/O requests per second for all Sun StorEdge 5310 NAS Appliance clients, select **System Activity > View Networking Activity** from the navigation panel.

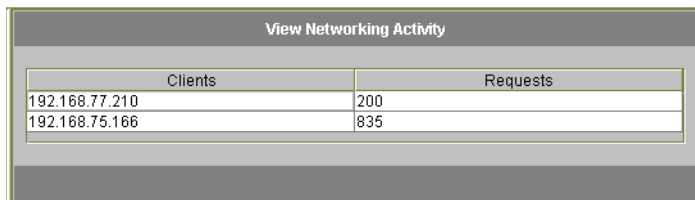


FIGURE 11-9 The View Networking Activity Panel

### Viewing System Activity

The Sun StorEdge 5310 NAS Appliance 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, in the navigation panel, select **System Activity > View System Activity**.

View System Activity		
Device	Load	Peak
CPU	25	32
Memory	13953	13953
aic1	0	0
aic2	0	0
emc1 (Intel Gigabit Copper)	3305	65461
emc2 (Intel Gigabit Copper)	59800	61007
ernf3 (Intel Gigabit Fiber)	0	0
ernf4 (Intel Gigabit Fiber)	0	0
fxp1 (Fast Ethernet)	72	72
ide1d1	2	2
isp1	16094	21031
isp1d000	0	0
isp3d021	0	0
isp1d002	27009	44895
isp3d023	16314	24495
isp2	441	927
isp2d000	546	1047
isp2d001	0	0
isp2d002	392	2109
isp4d023	0	0
isp3	8183	14484
isp4	25	26

**FIGURE 11-10** The View System Activity Panel

The system and network devices in the **View System Activity** panel are displayed as follows:

- **CPU**—Sun StorEdge 5310 NAS Appliance Central Processing Unit (CPU)
- **Memory**—Sun StorEdge 5310 NAS Appliance system Random Access Memory (RAM)
- **Port Aggregation x**—Port bond *x*
- **Controller x**—RAID controller *x*
- **dac010xx**—Logical Unit Numbers (LUNs) *xx*
- **PORTx**—Port *x*
- **Host Adapter x**—SCSI host adapter *x* (for tape backup device)

# Viewing Network (Port) Statistics

To view statistics about Sun StorEdge 5310 NAS Appliance network ports:

1. In the navigation panel, select **Network Configuration > Configure TCP/IP > Configure Network Adapters**.

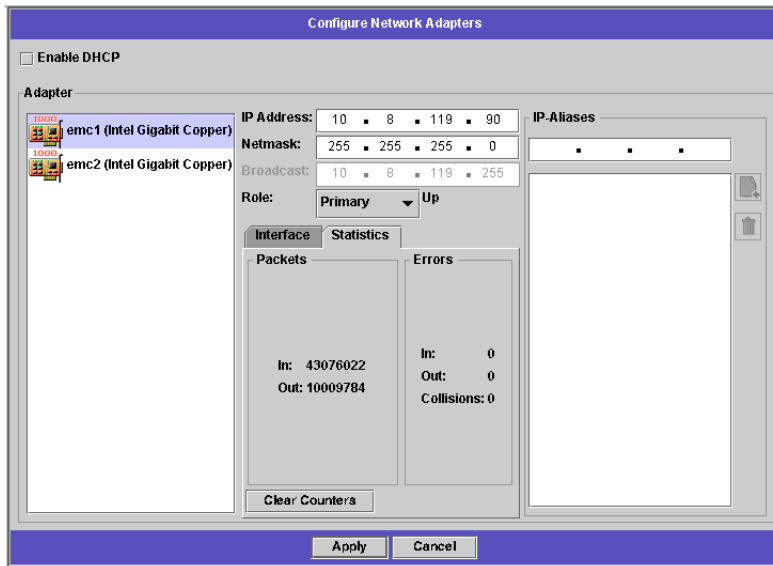


FIGURE 11-11 Viewing Network Statistics

2. Select the port from the Adapter list.

The **Interface** tab displays the following information:

- **Description**—Provides a description of the selected port.
- **H/W Address**—Shows the Hardware (H/W) or Media Access Control (MAC) address which is a unique address, in hexadecimal notation (hex), used by network software to distinguish this network card from other cards on the network. This address is encoded on the network card at the factory.
- **Speed**—Specifies the speed (Mb data/sec) at which data is transmitted over the network.
- **MTU**—Specifies the current MTU (Maximum Transmission Unit) 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 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.

3. Click the **Statistics** tab to display the following input/output information about the selected port:
  - **Packets In/Out**—The number of packets in/out (received/sent) by this port.
  - **Errors In/Out**—The number of errors in/out for this port.
  - **Collisions**—The number of transmission collisions for this port.

---

## Viewing Network Routes

The **View the Routing Table** panel allows you to view the routes by which packets are sent to the network and hosts. These routes consist of a destination network and a route entry reference.

### About Routing

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.

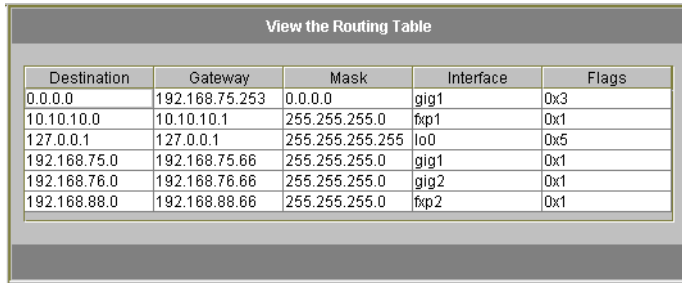
The following are some examples of route flags shown in the routing table:

- **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, in the navigation panel, select **Network Configuration > View the Routing Table**.



Destination	Gateway	Mask	Interface	Flags
0.0.0.0	192.168.75.253	0.0.0.0	gig1	0x3
10.10.10.0	10.10.10.1	255.255.255.0	fxp1	0x1
127.0.0.1	127.0.0.1	255.255.255.255	lo0	0x5
192.168.75.0	192.168.75.66	255.255.255.0	gig1	0x1
192.168.76.0	192.168.76.66	255.255.255.0	gig2	0x1
192.168.88.0	192.168.88.66	255.255.255.0	fxp2	0x1

**FIGURE 11-12** The View the Routing Table Panel

This screen displays the following information about each network route:

- **Destination**—This is the IP address of the route destination, and can refer to either a network or host. There should be one default route (designated 0.0.0.0), one loop-back route (designated 127.0.0.1), at least one network route, and at least one host route.
- **Gateway**—This is the gateway address through which the packets travel to the destination.
- **Mask**—This is the netmask for the destination network.
- **Interface**—This designates the interface type used to send packets over the network.
- **Flags**—The flags indicate the status of the route. Each type of status indication is represented by a number, in hexadecimal notation. See "About Routing" on page 169 for more information.

---

## Monitoring System Components

### UPS Monitoring

Use an Uninterruptible Power Supply (UPS) for your Sun StorEdge 5310 NAS Appliance unit. A properly sized UPS provides enough power for the Sun StorEdge 5310 NAS Appliance to log users off and shut down gracefully in the event of a power outage. It also serves to regulate or condition power coming into the unit, smoothing out power fluctuations.

---

**Note** – You must connect the UPS to the Sun StorEdge 5310 NAS Appliance system before you enable UPS monitoring. Otherwise, the monitoring system notifies you that there is a UPS failure. Also, the Sun StorEdge 5310 NAS Appliance does not support UPS management, only UPS monitoring. Refer to the *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide* for a picture showing the UPS port.

---

## UPS Monitoring Capability

Sun StorEdge 5310 NAS Appliance 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 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 UPS monitoring:

1. In the navigation panel, select **Monitoring and Notification > Enable UPS Monitoring**.

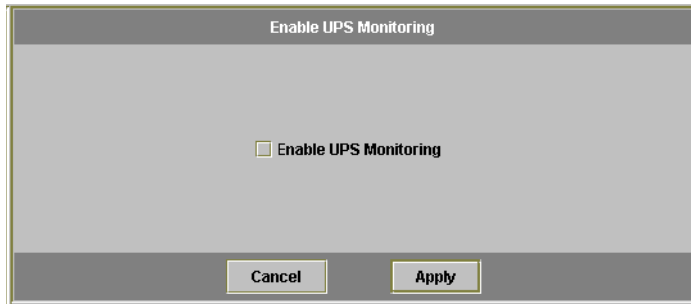


FIGURE 11-13 The Enabling UPS Monitoring Panel

2. Select the **Enable UPS monitoring**.
3. Click **Apply** to save your change.

## Viewing Controller Information

The read-only **View Controller Information** panel displays controller vendor, model, and firmware release.

To view controller vendor, model, and firmware release, select **RAID > View Controller Information** in the navigation panel.

## Viewing Mirroring Status

### Viewing Mirror Statistics

The Sun StorEdge 5310 NAS Appliance maintains a variety of network statistics for mirrored file volumes. These statistics are only available on the active server for each mirrored file volume.

1. From the navigation panel, select File Replicator > View Mirror Statistics.

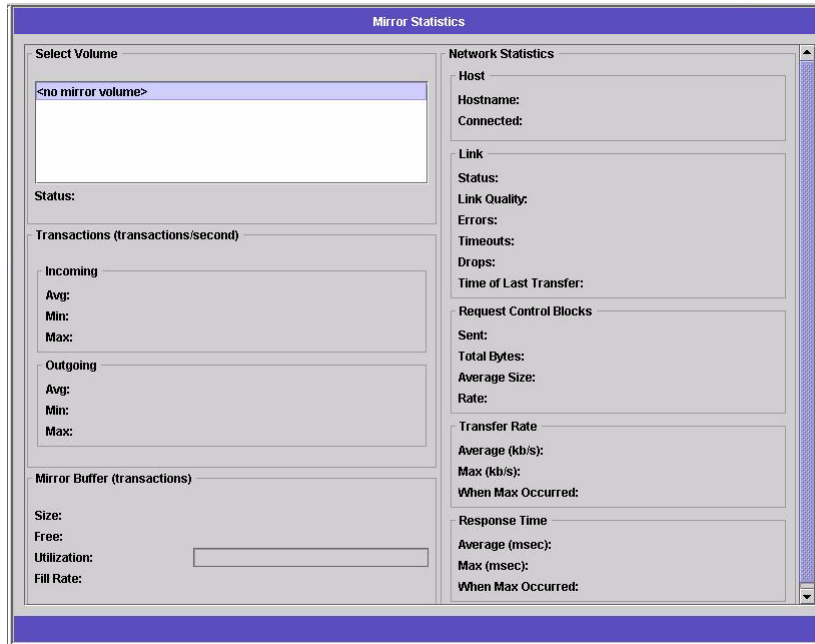


FIGURE 11-14 The Mirror Statistics Panel

2. Select the file volume you want from the Select Volume list. The Sun StorEdge 5310 NAS Appliance displays the following information for that mirrored file volume:
  - **Status**—This field shows the status of the mirror. For definitions of status indicators, please refer to "Mirror Status States" on page 174.
  - **Incoming Transactions**—This section shows the following statistics for the selected file volume:
    - **Average**—The average number of transactions per second traveling into the active server.
    - **Minimum**—The lowest number of transactions per second that has traveled into the active server. The date and time this minimum occurred is shown on the right.
    - **Maximum**—The highest number of transactions per second that has traveled into the active server. The date and time this maximum occurred is shown on the right.
  - **Outgoing Transactions**—This section shows the following statistics for the selected file volume:
    - **Average**—The average number of transactions per second traveling from the active server to the mirror server.

- **Minimum**—The lowest number of transactions per second that has traveled from the active server to the mirror server. The date and time this minimum occurred is shown on the right.
- **Maximum**—The highest number of transactions per second that has traveled from the active server to the mirror server. The date and time this maximum occurred is shown on the right.
- **Mirror Buffer**—This section shows the status of the mirror buffer as follows:
  - **Size**—The size of the mirror buffer.
  - **Free**—The number of transactions left in the mirror buffer.
  - **Utilization**—The percentage of transactions used in the mirror buffer.
  - **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. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, thus filling up the buffer.
- **Network Statistics**—This section shows the network statistics of the mirror buffer as follows:
  - **Host**—The hostname and connection status for the mirror buffer.
  - **Link**—The status, quality, and other link statistics for the mirror buffer.
  - **Request Control Blocks**—The number of control blocks sent, the total bytes sent, and the average size and rate.
  - **Transfer Rate**—The average rate at which transfers occur, the maximum, and the time when the maximum transfer occurred.
  - **Response Time**—The average response time, the maximum response time, and the time when the maximum response time occurred.

## 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.



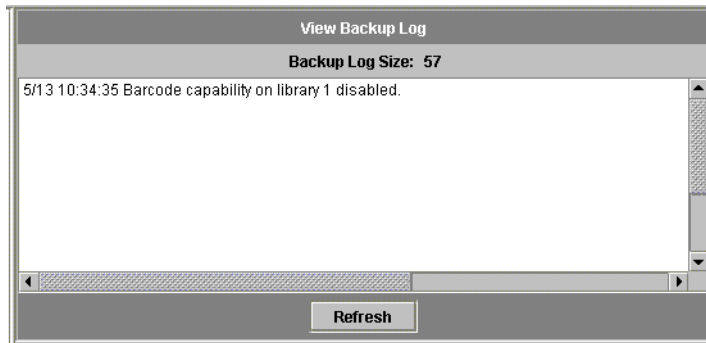
---

# Viewing Backup Job Status

## Viewing the Backup Log

The backup log displays a complete list of events that have occurred in system backup processes and includes the date, time, and a description of each event. Scroll upwards to view earlier backup events.

To view the log, select **System Backup > Manage Backup Jobs > View Backup Log**.

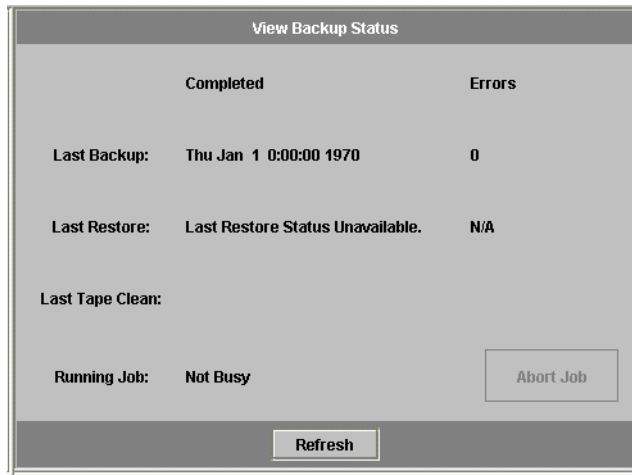


**FIGURE 11-15** The View Backup Log Panel

The total size of the file is shown at the top of the screen. Click **Refresh** to refresh the log file display.

## Viewing Job Status

To display the status of system backup processes, select **System Backup > Manage Backup Jobs > View Backup Status**.



**FIGURE 11-16** The View Backup Status Panel

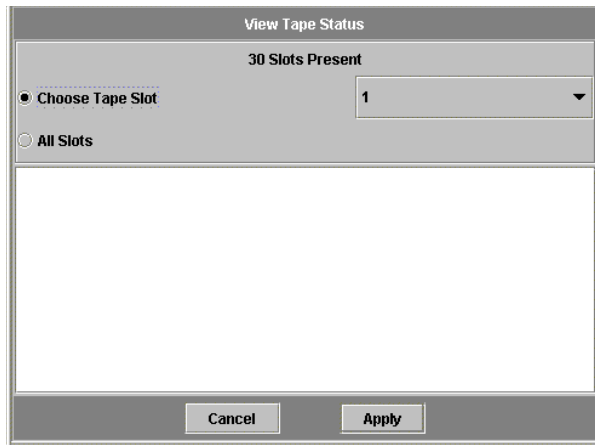
This screen shows the most recent backup, restore, and cleaning processes. If a backup or restore process is running, the **Abort Job** button is enabled. Click this button to halt a running process and check the system events panel for confirmation that the job was canceled. Allow several minutes for the cancellation to take effect.

## Viewing Tape Status

The **View Tape Status** panel provides information about backup tapes in the tape device. You cannot view this data when a backup, restore, or head cleaning process is in progress.

To display the status of tapes in the local backup device:

1. In the navigation panel, select **System Backup > Manage Backup Jobs > View Tape Status**.



**FIGURE 11-17** The View Tape Status Panel

2. **Select the tape information you want to view.**
  - To view information about a particular tape, select the **Choose Tape Slot** option. Then select the slot corresponding to the tape you want to view from the list.  
Slot numbering in this screen starts with 1. However, individual tape backup device slot numbering may vary. If the slot numbering in your tape device starts with 0 (zero), select slot 1 in this screen to view information about slot 0 in your tape device.
  - To view information about all tapes in the tape device, select **All Slots**.  
The system takes 1-2 minutes per slot to retrieve tape information, which is displayed in the area at the bottom of the screen. Selecting **All Slots** greatly increases the time it takes to get the information. The tape device cannot retrieve slot information while a backup, restore, or head cleaning process is in progress.
3. **Click Apply to start the tape discovery.**



# System Maintenance

---

This chapter describes maintenance functions.

---

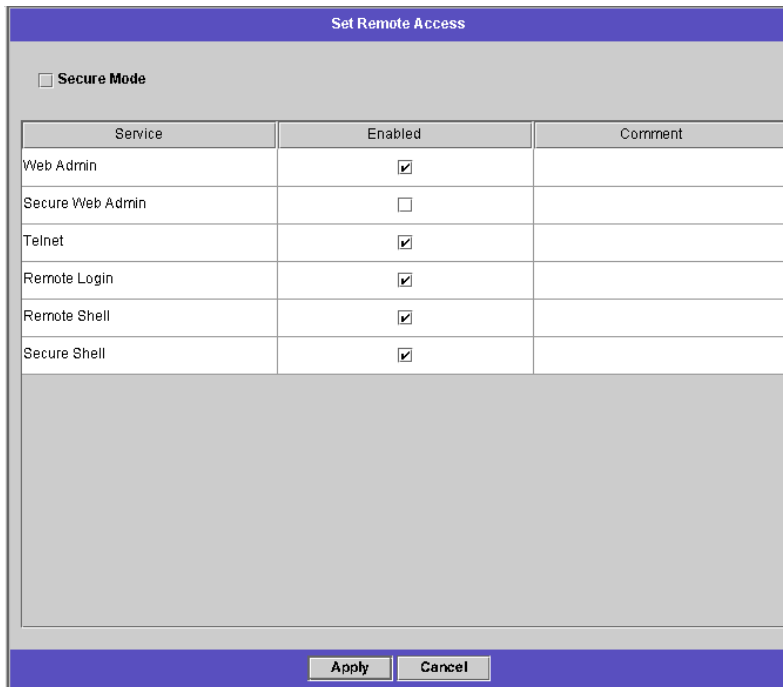
## Setting Remote Access Options

Sun StorEdge 5310 NAS Appliance security features include the ability to set remote access options. You can enable or disable network services used to remotely access the Sun StorEdge 5310 NAS Appliance. 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 http, and Secure Shell (ssh).

To set remote access security:

1. In the navigation panel, select **System Operations > Set Remote Access**.



The screenshot shows the 'Set Remote Access' configuration window. At the top, there is a checkbox for 'Secure Mode'. Below it is a table with three columns: 'Service', 'Enabled', and 'Comment'. The table lists several services with their corresponding 'Enabled' checkboxes. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Service	Enabled	Comment
Web Admin	<input checked="" type="checkbox"/>	
Secure Web Admin	<input type="checkbox"/>	
Telnet	<input checked="" type="checkbox"/>	
Remote Login	<input checked="" type="checkbox"/>	
Remote Shell	<input checked="" type="checkbox"/>	
Secure Shell	<input checked="" type="checkbox"/>	

**FIGURE 12-1** The Set Remote Access Panel

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**, check 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**, you must restart the server for the settings to go into effect. Refer to "Shutting Down the Server" on page 183.

---

# 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.

You can set up three types of users:

- **Administrators** who have the username “admin” and use the same password used by GUI clients.  
The administrator has “root” access to all volumes, directories, and files on the Sun StorEdge 5310 NAS Appliance. The administrator’s home directory is defined as “/”.
- **Users** who have a username and a password specified in the local password file or on a remote NIS, NIS+, or LDAP name server.  
The user has access to all 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 login with the username “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.

---

To set up FTP users:

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

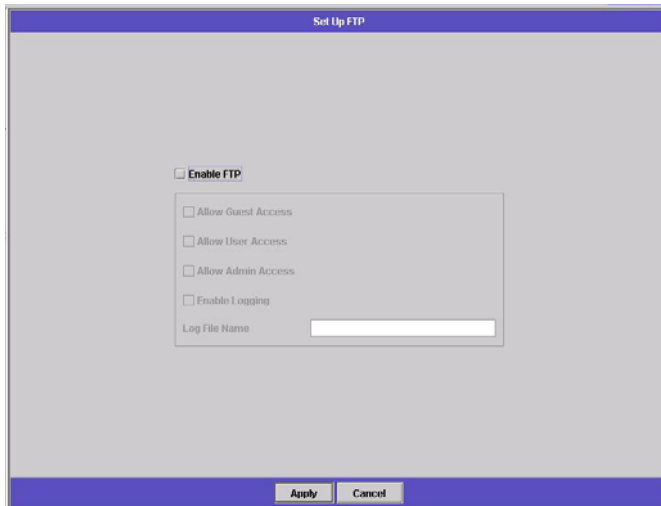


FIGURE 12-2 The Set Up FTP Panel

2. Check the Enable FTP checkbox.
3. Select the type of FTP access by checking the appropriate checkbox(es):
  - 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 NIS, NIS+, or LDAP name server.

---

- Allow Admin Access enables root access to those in possession of the Sun StorEdge 5310 NAS Appliance administrative password (use with caution).

---

**Note** – A “root” user is a user with UID equal to 0 and the special Sun StorEdge 5310 NAS Appliance user “admin”.

---

4. To enable logging, check the Enable Logging checkbox and specify the log file name.
5. Click Apply to save settings.



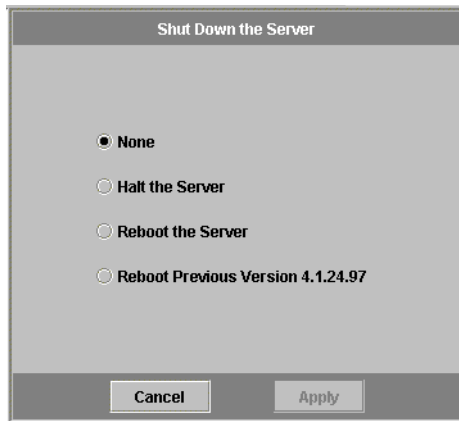
---

# Shutting Down the Server

The **Shut Down the Server** panel allows you to shut down, halt, or reboot the server (See "Shutting Down the System" on page 256 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**.



**FIGURE 12-3** The Shut Down the Server Panel

2. Select one of the following three options:
  - **Halt the Server**—Click this option to shut down the server.
  - **Reboot the Server**—Click this option to shut down and restart the server.
  - **Reboot Previous Version**—Click this option to shut down and restart the server with the previously loaded version of software. Use this option if, for example, you encountered problems while upgrading the software. This option lets you restart with the last software used before the upgrade.



---

**Caution** – Check with Technical Support before selecting the Reboot Previous Version option.

---

3. Click **Apply**.

---

# Failover

## About Head Failover

A Sun StorEdge 5310 Cluster is a dual-head system consisting of a pair of active-active server heads that share access to a pair of RAID controllers and several different networks. The RAID controllers are connected to each head through independent SCSI or fibre controllers. A dedicated heartbeat cable connects the two heads and allows each head to monitor the other head's health status.

In normal operation, each head operates independently, with responsibility for a subset of the disk volumes. If one head suffers a hardware failure that renders a data path unavailable, the working head automatically takes ownership of the LUNs formerly managed by the failed head. All operations of the failed head, including RAID volume ownership and network interface addressing, are transferred to the working head. This is known as **head failover**.

Each primary port configured on a Sun StorEdge 5310 Cluster head can have up to four unique alias IP addresses. If one head fails, the other head takes over both the primary IP address and the alias IP addresses of the failed head.

---

**Note** – When you enable head failover, DHCP is automatically disabled.

---

Following a cluster failover, client operations using NFS/UDP transfer immediately, while NFS/TCP requires a reconnect which is performed transparently in the context of a NFS retry. CIFS also requires a reconnect, although different applications may do so transparently, notify the user, or require user confirmation before proceeding.

You initiate the recovery process, known as *failback*, when you have repaired the failed head and brought it back online. See "Initiating Failback" on page 186.

## About Controller Failover

Controller failover differs from head failover in that it involves redundant RAID/SCSI controllers rather than redundant server heads. In the event of RAID controller failure, controller failover allows a working RAID controller to take ownership of RAID volumes formerly managed by the failed controller.

In the event of a controller failure, the redundant controller takes control of the RAID set and drives formerly controlled by the failed controller. As in head failover, when the failed controller is replaced or repaired, you can define which RAID sets and drives are controlled by each controller.

## Configuring Failover

The **Enable Failover** panel allows you to enable head failover for the dual-head Sun StorEdge 5310 Cluster or RAID controller failover for the single-head Sun StorEdge 5310 NAS Appliance.

### Enabling Controller Failover

Controller failover occurs automatically when a RAID controller fails. The working controller temporarily manages the LUNs that were managed by the failed controller. When the failed head or RAID controller is brought back online, proceed to **Fault Tolerance > Recover** to begin the recovery process. For more information, refer to "Initiating Failback" on page 186.

---

**Note** – Controller failover is enabled by default, and cannot be disabled.

---

### Enabling Head Failover

In the event of a head failure, failover causes the working head to take temporary ownership of the IP address(es) and LUN(s) formerly managed by the failed head.

To enable head failover:

1. In the navigation panel, select **Fault Tolerance > Enable Failover**.

The screenshot shows the 'Enable Failover' configuration window. At the top, the title is 'Enable Failover'. Below the title, there is a checked checkbox labeled 'Automatic Failover'. Underneath, the 'Head Status' is shown as 'NORMAL'. A section titled 'Link Failover' contains an unchecked checkbox labeled 'Enable Link Failover'. Below this, there are two input fields: 'Down Timeout:' with the value '60' and 'Restore Timeout:' with the value '60'. A section titled 'Partner Configuration' contains three input fields: 'Name:' with the value 'p2', 'Gateway:' with three asterisks, and 'Private IP:' with the value '10 + 10 + 10 + 2'. At the bottom of the window are two buttons: 'Cancel' and 'Apply'.

**FIGURE 12-4** The Enable Failover Panel

2. Click the **Automatic Failover** checkbox.
3. Select the **Enable Link Failover** checkbox. This function ensures that head failover occurs when the primary link of one head fails. Then 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.
4. Click **Apply**.

---

## Initiating Failback

You must manually initiate recovery of your Sun StorEdge 5310 NAS Appliance or Sun StorEdge 5310 Cluster system after it has undergone head or controller failover.



---

**Caution** – Make sure that the failed head is fully operable before attempting recovery.

---

To configure head or controller failback:

1. In the navigation panel, select **Fault Tolerance > Recover**.

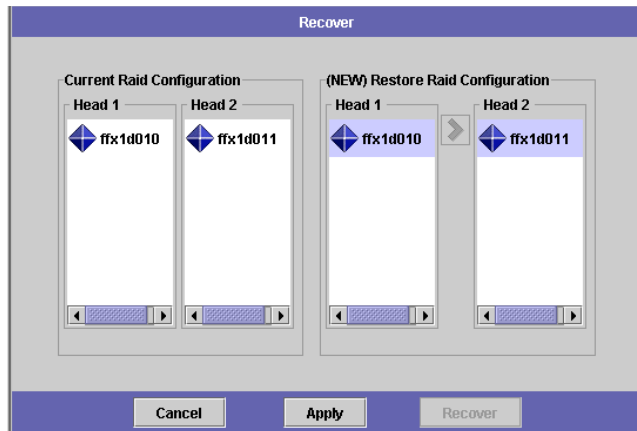


FIGURE 12-5 The Recover Panel for Head Failback

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

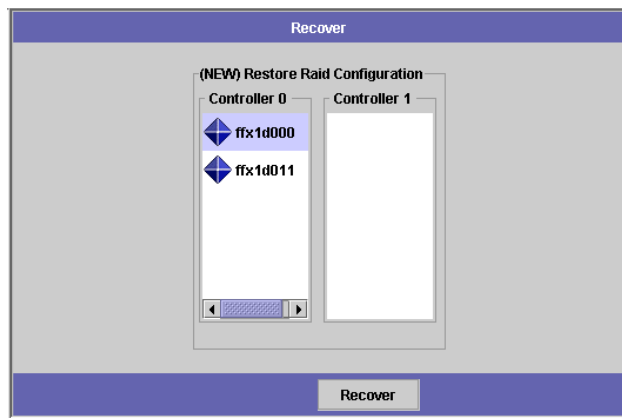


FIGURE 12-6 The Recover Panel for Controller Failback

3. For controller recovery, in the RAID list select the RAID set you are recovering.
  - The **Controller 0** list identifies LUN mapping for Controller 0.
  - The **Controller 1** (partner) list identifies LUN mapping for Controller 1.
4. Click **Recover**. The server rearranges the LUN mapping to reflect the configuration shown on the screen.

---

# File Checkpoints

## 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.

---

An enormous amount of space and system memory is required for checkpoints. The more checkpoints there are on a system, the greater the potential effect on system performance.

To use File Checkpoints, you must first go to the **Edit Properties** panel (in the **File Volume Operations** folder) to enable checkpoints. Then create individual checkpoints in the **Manage Checkpoints** panel (in the **File Volumes > Configure Checkpoints** folder), or make a schedule in the **Schedule Checkpoints** panel.

## Creating File Checkpoints

You can choose whether to schedule a checkpoint or create one immediately. Refer to "Scheduling File Checkpoints" on page 190 for information on setting up a regular checkpoint schedule.

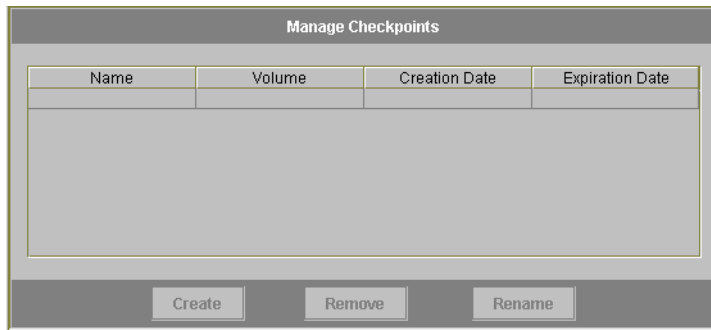
In the **Manage Checkpoints** panel, you can create immediate checkpoints as well as rename and remove existing ones. Unlike scheduled checkpoints, which are created at a pre-determined day and time, you can create immediate checkpoints in this screen at any time.

## Creating a Checkpoint

Using the **Manage Checkpoints** panel, you may configure a checkpoint to occur immediately instead of on a time schedule. There is no maximum number of checkpoints that you can schedule.

To create a new checkpoint manually:

1. In the navigation panel, select **File Volume Operations > Edit Properties**.
2. Select the volume for which you want to create a checkpoint in the **Volume Name drop-down list**.
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**.



**FIGURE 12-7** The Manage Checkpoints Panel

5. To create a new checkpoint, click **Create**.

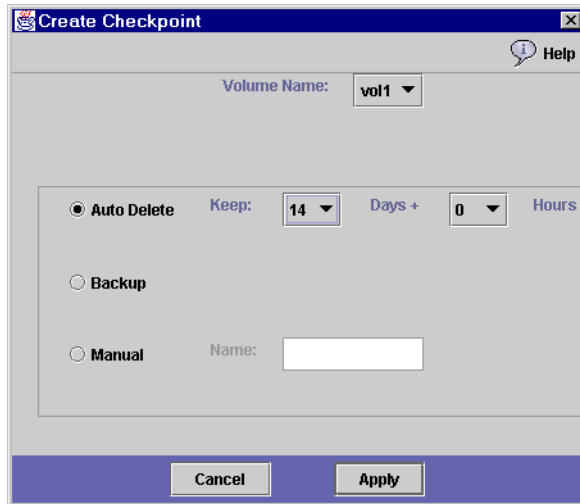


FIGURE 12-8 The Create Checkpoint Dialog Box

6. Select the **Volume Name** for which you want to create a checkpoint from the drop-down list.
7. Select one of the following checkpoint options:
  - **Auto Delete**—Select **Auto Delete** to automatically remove the checkpoint after the number of **Keep Days** and **Keep Hours** have elapsed. In this option the name of the checkpoint is automatically assigned by the system. If you select this option, select the number of days and hours the checkpoint should be retained.
  - **Backup**—In this option, the default name of the checkpoint is **Backup**. The checkpoint is used for local backups of the Sun StorEdge 5310 NAS Appliance file system. The checkpoint is not automatically deleted after a specific time period.
  - **Manual**—If you want to name the checkpoint something other than **Backup**, select this option. Then enter the name in the **Name** field. The checkpoint is not automatically deleted after a specific time period.
8. Click **Apply** to create the checkpoint.

## 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 time(s) 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.

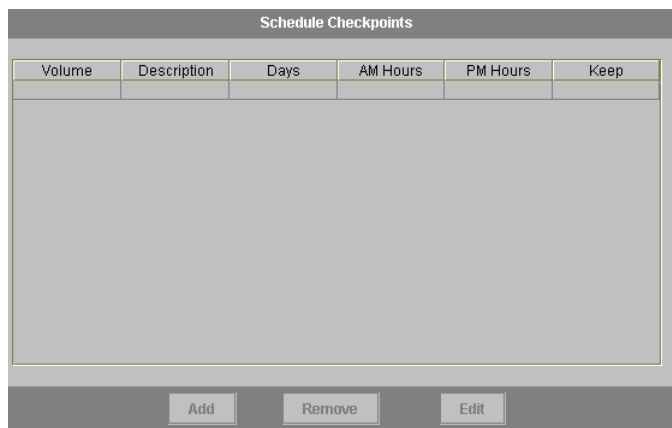


## Adding an Entry to the Checkpoint Schedule

The **Schedule Checkpoints** panel displays a table of all scheduled checkpoints for the system. Adding a schedule line causes the system to automatically set up a checkpoint for the times and dates requested. There is no maximum number of checkpoints that you can schedule.

To add a checkpoint to the schedule:

1. Enable checkpoints for the file volume.
  - a. In the navigation panel, select **File Volume Operations > Edit Properties**.
  - b. Select the volume for which you want to add a checkpoint in the **Volume Name drop-down list**.
  - c. Be sure there is a check mark () in the **Enable Checkpoints** box. If not, select the box and click **Apply**.
2. In the navigation panel, select **File Volume Operations > Configure Checkpoints > Schedule Checkpoints**.



**FIGURE 12-9** The Schedule Checkpoints Panel

3. To add a checkpoint to the schedule, click Add.

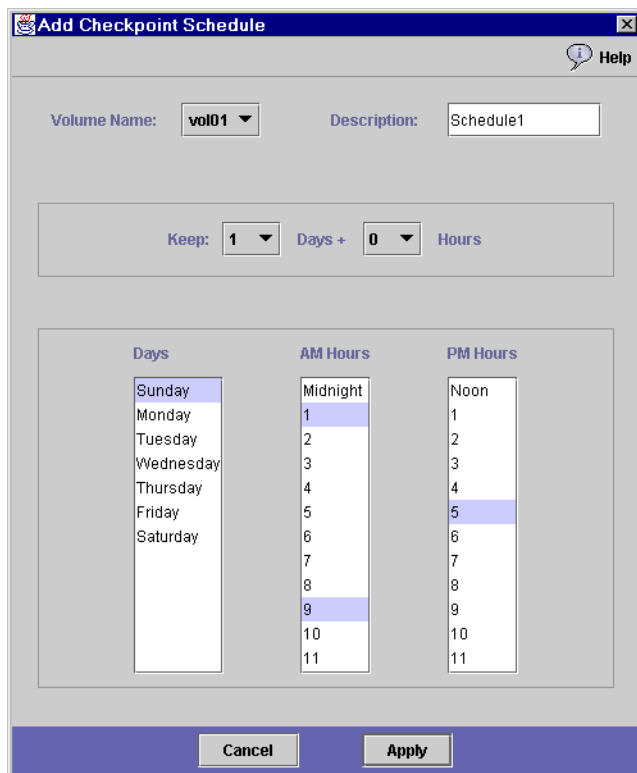


FIGURE 12-10 The Add Checkpoint Schedule Dialog Box

4. Select the file volume for which you are scheduling checkpoints.
5. 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.”
6. Select the number of days and hours to retain the checkpoint in the Keep Days + Hours drop-down boxes.
7. 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.
8. 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.

9. In the PM Hours list, select the time(s) 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.
10. Click Apply to save your changes.

## Editing an Entry in the 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.

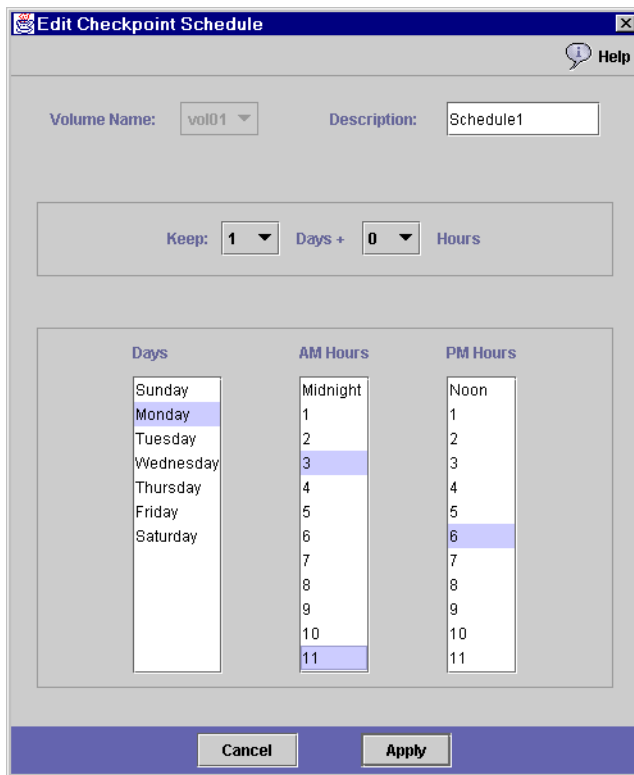


FIGURE 12-11 The Edit Checkpoint Schedule Dialog Box

3. The information shown on this screen is identical to that in the Add Checkpoint Schedule dialog box, except that you cannot change the volume name. Edit the relevant information. For more information, see "Adding an Entry to the Checkpoint Schedule" on page 191.
4. Click **Apply** to save your changes.

## Removing an Entry from the Checkpoint Schedule

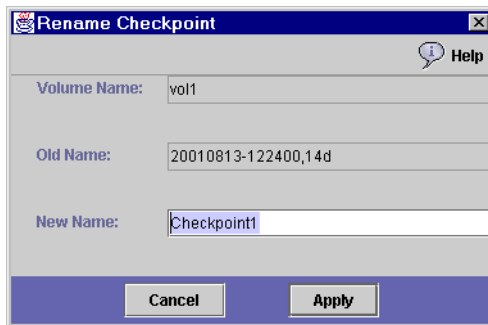
To remove a schedule line:

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 Sun StorEdge File Checkpoint

To rename a checkpoint in the **Manage Checkpoints** panel:

1. In the navigation panel, select **File Volume Operations > Configure Checkpoints > Manage Checkpoints**.
2. Select the checkpoint you want to rename, and click **Rename**.



**FIGURE 12-12** The Rename Checkpoint Dialog Box

The **Volume Name** and **Old Name** fields are read-only.

3. Enter the New Name for the checkpoint.



---

**Caution** – If you rename an auto-delete checkpoint to a common name, the checkpoint will no longer auto-delete.

---

4. Click **Apply** to save your changes.

## Removing File Checkpoints

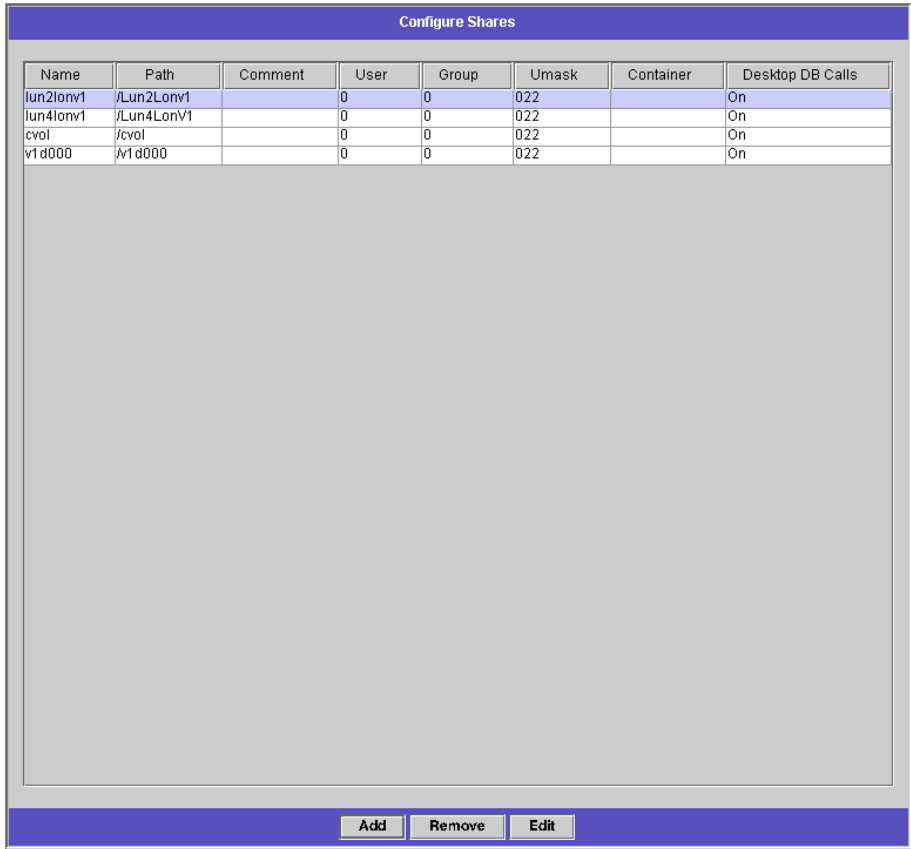
To remove a checkpoint from the **Manage Checkpoints** panel:

1. In the navigation panel, select **File Volume Operations > Configure Checkpoints > Manage Checkpoints**.
2. Select the checkpoint you want to remove, then click **Remove**.

## Sharing File Checkpoints

Checkpoints can be shared, allowing users to access the data that was current when the checkpoint was created.

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



Name	Path	Comment	User	Group	Umask	Container	Desktop DB Calls
lun2lonv1	/Lun2Lonv1		0	0	022		On
lun4lonv1	/Lun4LonV1		0	0	022		On
cvol	/cvol		0	0	022		On
v1d000	/v1d000		0	0	022		On

Buttons: Add, Remove, Edit

FIGURE 12-13 The Configure Shares Panel

2. Click Add.

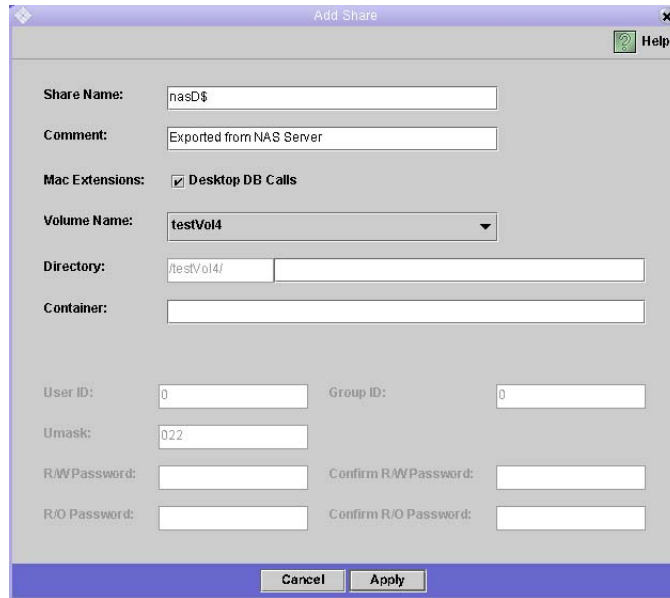


FIGURE 12-14 The Add Share Dialog Box

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. The Mac Extensions option is checked by default.
5. Click the Volume Name drop-down list box and select the checkpoint volume from the list. Checkpoint volumes have the “.chkpnt” extension
6. Leave the Directory field blank.
7. If ADS is enabled and configured, type an ADS context in the Container text box.
8. The following fields and options are grayed out if Sun StorEdge 5310 NAS Appliance is configured for NT Domain mode. Otherwise complete them as follows:
  - a. Type 0 in the User box.
  - b. Type 0 in the Group box.
  - c. Leave the R/W Password and R/O Password boxes blank. Checkpoint volumes are read only.
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.

1. Using a network station, click the Windows Start menu.

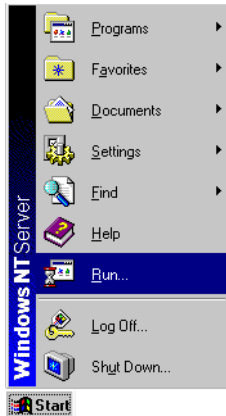


FIGURE 12-15 The Windows Start Menu

2. Select Run.

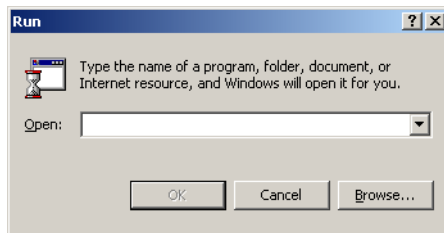


FIGURE 12-16 The Run Dialog Box

3. In the Run dialog box, type the Sun StorEdge 5310 NAS Appliance server IP address and checkpoint sharename. For example, type "`\\xxx.xxx.xxx.xxx\sharename`".
4. Click OK.



# Backup and Restore

## Setting Up NDMP

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.

---

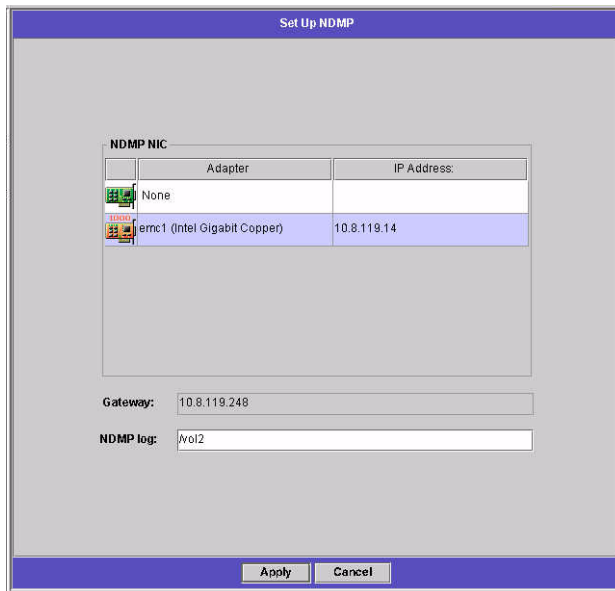
**Note** – The backup administration application should be configured for logon with the user name “administrator” and the password used by the console administrator (command line interface).

---

NDMP is not required to run local backups.

To set up NDMP:

1. In the navigation panel, select System Backup > Set Up NDMP.



**FIGURE 12-17** The Set Up NDMP Panel

2. Select the NDMP NIC to be used for data transfer to the backup tape drive.

3. The Gateway address 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.

---

## Running a Head Cleaning

To view information about the last head cleaning or to set up the next head cleaning for the local tape device:

1. In the navigation panel, select System Backup > Assign Cleaning Slot.

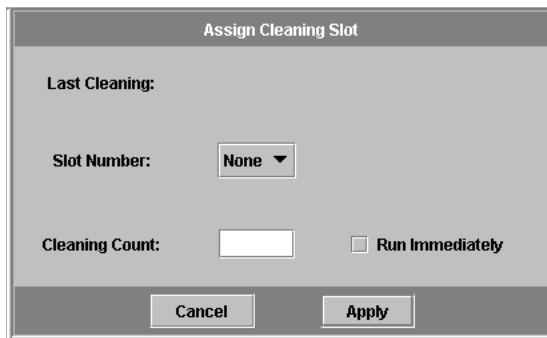


FIGURE 12-18 The Assign Cleaning Slot Panel

2. Select the Slot Number that contains the cleaning tape for this head cleaning.  
Slot numbering in this screen starts with 1. However, individual tape backup device slot numbering may vary. If the slot numbering in your tape device starts with 0 (zero), select slot 1 in this screen to view information about slot 0 in your tape device.
3. Assign a Cleaning Count number to keep track of the number of times a cleaning tape is used for head cleaning.  
Use a cleaning tape no more than 10 times before discarding it. This number incrementally increases every time a head cleaning takes place.
4. To run the head cleaning job now, select the Run Immediately checkbox to begin the tape cleaning with the specified slot number and cleaning count.
5. Click Apply to save your changes. If you selected the Run Immediately checkbox, the cleaning job begins at this time.

---

# Updating Sun StorEdge 5310 NAS Appliance Software

Contact Sun Microsystems Technical Support to obtain the appropriate update files for your Sun StorEdge 5310 NAS Appliance system and configuration. Once you have the files, use the **Update Software** panel to update the Sun StorEdge 5310 NAS Appliance software.



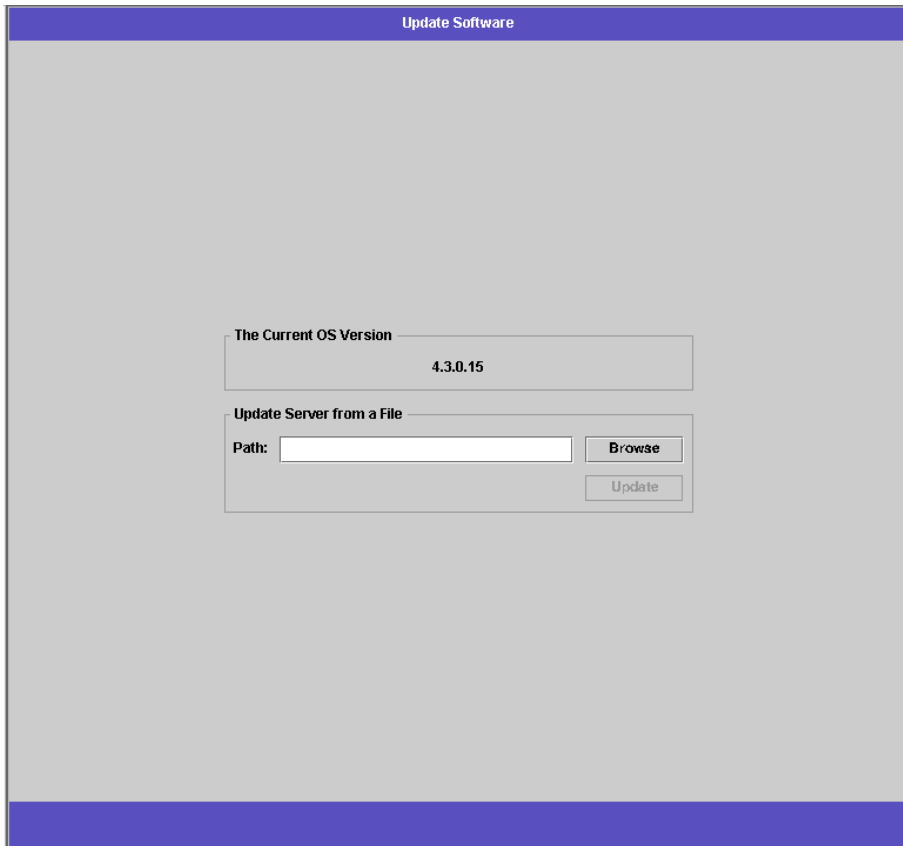
---

**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.

---

To update software:

1. In the navigation panel, select System Operations > Update Software.



**FIGURE 12-19** The Update Software Panel

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 No to continue without rebooting. The update does not take effect until the system is rebooted.

## Console Administration

---

The console is the alternative method to Web Administrator for managing the Sun StorEdge 5310 NAS Appliance server. You may use a number of protocols such as Telnet, SSH, RLogin, etc. to connect to the Sun StorEdge 5310 NAS Appliance administrator console as long as the application you use has an ANSI-compatible terminal emulator. In this chapter we use the Telnet protocol because it is readily available in MS Windows.

---

**Note** – Remote access security settings may need to be altered to access the command line interface. Refer to "Setting Remote Access Options" on page 179 for remote access details.

---

---

## Accessing The Console Administrator

In this example Windows Telnet is used; however, you may use another protocol as long as it has an ANSI-compatible terminal emulator.

To access Windows Telnet:

1. **Click Start from your desktop taskbar.**
2. **Select Run.**

3. In the Run window, enter **Telnet** and click **OK**.

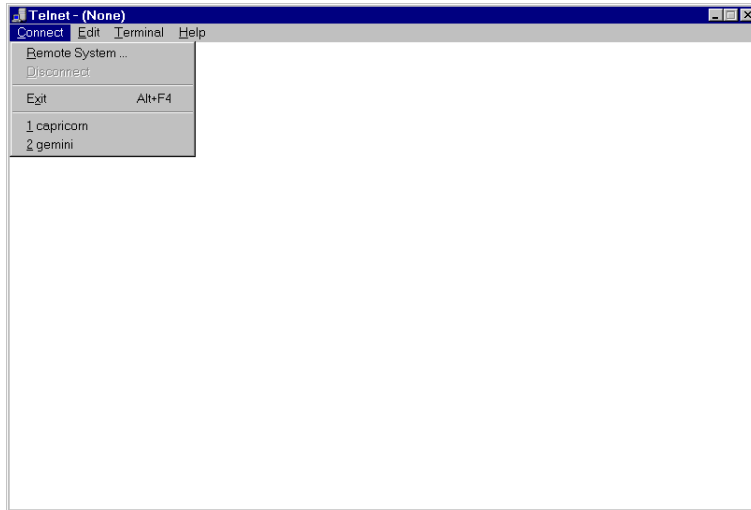


FIGURE A-1 The Telnet Screen

4. From the **Connect** menu, select **Remote System**.

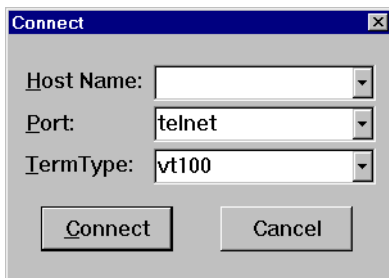


FIGURE A-2 The Connect Dialog Box

5. In **Host Name**, enter the server name or IP address.

6. In **Port**, select **Telnet**.

7. In **TermType**, enter **vt100**.

8. Click **Connect**. If administrative access is password-protected, you are asked for the password.

Once connected, the Telnet screen displays the following command line prompt:

```
connect to (? for list) ? [menu] █
```

**FIGURE A-3** The Telnet Connection Prompt

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 Command Line Interface

At the Telnet connection prompt (displayed above):

1. Type **admin** and press **Enter**.
2. Then type the **administrative password** and press **Enter**.

The command line prompt appears. You can type a command or 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

This section describes the components of the Telnet screen used for setting up and maintaining your system.

## Basic Guidelines

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** screen.
- 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.

## Key Descriptions

The following keys are used to edit screen fields:

**TABLE A-1** Active Screen Keys

Backspace, Delete, Ctrl+H	Deletes the previous character
Ctrl+U	Deletes the entire field
Enter, Ctrl+M, Ctrl+J, Ctrl+I, Tab	Entry is complete and the cursor proceeds to the next field
Esc	Exits the screen with no change

If you do not want to change a field value, press **Enter** and the cursor moves to 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 space bar to scroll through the extension lists.

Select the menu item by pressing the corresponding letter or number.

```
wgs67-16                               Menu
-----
Operations                               | Configuration | Access Control
1. Activity Monitor                    | A. Host Name & Network | K. Admin Access
2. Show Log                            | B. Timezone, Time, Date | L. Volume Access
3. Lock Console                        | C. Drive Letters      | M. Trusted Hosts
4. Licenses                            | D. Disks & Volumes    |
                                         | E. Users              | Extensions
                                         | F. Hosts              | U. Language Selection
                                         |                       | V. EMAIL Configuration
                                         | H. DNS & SYSLOGD     | W. ADS Setup
                                         | I. NIS & NIS+        | X. CIFS/SMB Configuration
0. Shutdown                            | J. NS Lookup Order   | Y. RDATE time update
-----
Version 4.02 M38 (Build 149)           --SPACE more extensions--

+-----+
| |Press the number or letter that corresponds to the|
| | menu item you want to use                       |
| |                                                 |
+-----+
ESC to exit menu                               Sun Microsystems, Inc.
```

**FIGURE A-4** The Main Menu

Click the **spacebar** to view more options under the **Extension** lists.

```
London                               StorEdge 5310 NAS Menu
-----
Operations                               | Configuration | Access Control
1. Activity Monitor                    | A. Host Name & Network | K. Admin Access
2. Show Log                            | B. Timezone, Time, Date | L. Volume Access
3. Lock Console                        | C. Drive Letters      | M. Trusted Hosts
4. Licenses                            | D. Disks & Volumes    |
                                         | E. Users              | Extensions
                                         | F. Hosts              | U. Tape Backup
                                         |                       | V. Company Information
                                         | H. DNS & SYSLOGD     | W. Diagnostics
                                         | I. NIS & NIS+        | X. NDMP Setup
0. Shutdown                            | J. NS Lookup Order   | Y. LUN Paths
-----
Version 4.03 M0                       --SPACE more extensions--

+-----+
| |Press the number or letter that corresponds to the|
| | menu item you want to use                       |
| |                                                 |
+-----+
ESC to exit menu                               Sun Microsystems, Inc.
```

**FIGURE A-5** The Extensions List

---

# Configuration Backup



---

**Caution** – The Sun StorEdge 5310 NAS Appliance stores redundant copies of the configuration information, but you must make a backup copy in case of system failure.

---

To back up the configuration information:

1. Follow instructions for "Accessing the Command Line Interface" on page 205.



---

**Caution** – Use commands carefully to avoid unintended results.

---

2. At the command line enter `load unixtools`
3. Then type `cp -r v /dvol/etc <backup path>` where *<backup path>* is the full path, including volume name, of the desired directory location of the configuration files 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

## Configuring TCP/IP

To setup the host server name, the IP address, and the transmit rate:

1. From the Configuration menu, select Host Name & Network.

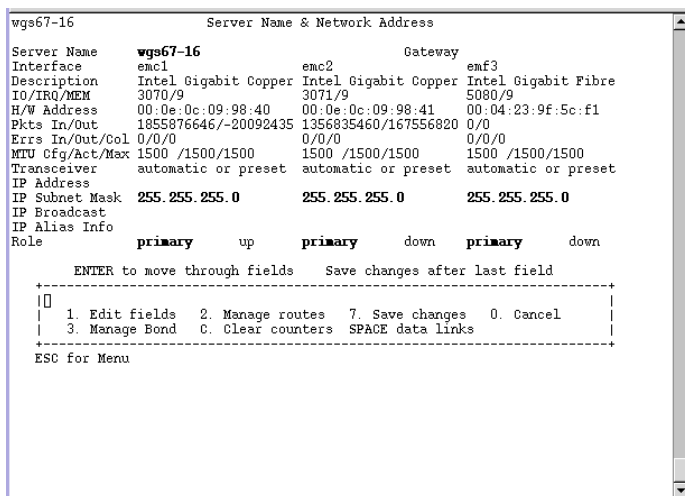


FIGURE A-6 Configuring the Host Name and Network Information

2. Select 1. Edit fields.
3. Enter 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

This screen allows you to change the administrator password. Always protect your servers with passwords.

To modify:

1. From the Access Control menu, select Admin Access.

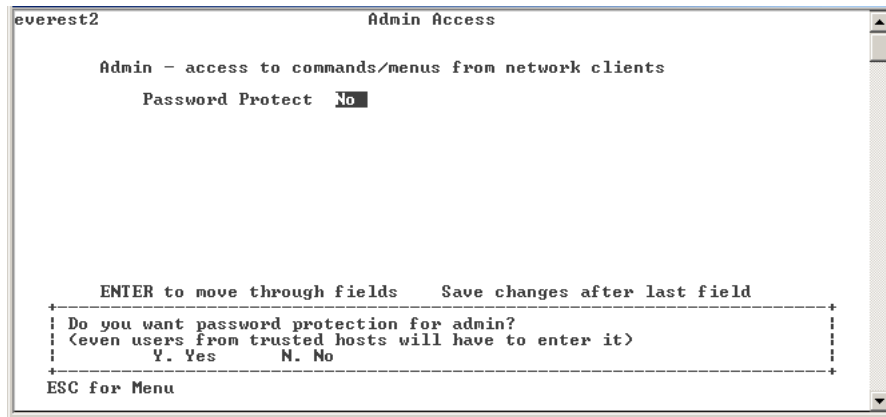


FIGURE A-7 The Admin Access Screen

2. Select Y. Yes to enable password protection, or N. No to disable it.

---

**Note** – Always protect your Sun StorEdge 5310 NAS Appliance server 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

## Setting the Time Zone, Time, and Date

Use the **Timezone, Time, Date** menu option to change time zone, time, and date set on the Sun StorEdge 5310 NAS Appliance server. The real-time clock on the mainboard keeps track of local time.

---

**Note** – The first time you set the time and date on the Sun StorEdge 5310 NAS Appliance 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.

---

To set up time:

1. From the Configuration menu, select **Timezone, Time, Date**.

```
London          StorEdge 5310 NAS Timezone, Time, & Date
Timezone       EST
Minutes west of GMT 300
Daylight time   Yes

Current        New
Date           12/20/2004
Time           18:54

ENTER to move through fields   Save changes after last field
+-----+
|[]What is the local timezone?  |
| 1. Other 5. Eastern 6. Central 7. Mountain 8. Pacific |
+-----+
ESC for Menu
```

**FIGURE A-8** The Timezone, Time, Date Screen

2. Select the appropriate timezone, 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:  
20021001 equals October 1, 2002
5. Type the current time, then press Enter. The system uses a twenty-four hour clock:  
1300 equals 1:00 p.m.
6. Select 7. Save changes.

---

**Note** – If this is the first time you have set the time and date on the Sun StorEdge 5310 NAS Appliance, this will set the secure clock to the same time and date. Make sure you set the time and date accurately as you can only set the secure clock once.

---

## Setting Time Synchronization

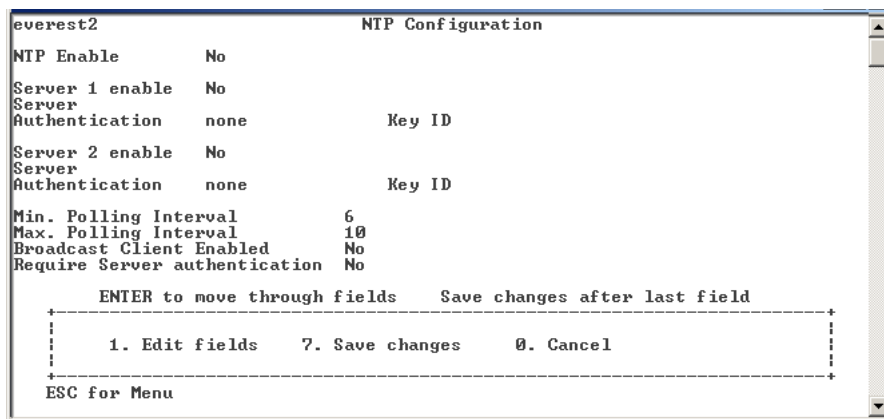
You can configure the Sun StorEdge 5310 NAS Appliance to synchronize its time with either NTP protocol or an RDATE server.

### *Setting Up Network Time Protocol (NTP)*

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.

To set up NTP:

1. From the Extensions menu, select NTP Configuration.



**FIGURE A-9** The NTP Configuration Screen

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 StorEdge 5310 NAS Appliance polls for the current time, then press Enter.
6. Choose the type of Authentication to use, either 0. none and 1. symmetric-key. Symmetric key authentication support lets the Sun StorEdge 5310 NAS Appliance verify that the server is known and trusted by using a key and key ID. The NTP server and Sun StorEdge 5310 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 StorEdge 5310 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 RDATE Time Synchronization

RDATE servers are normally present on UNIX systems and allow you to synchronize Sun StorEdge 5310 NAS Appliance server time with RDATE server time.

To set up the RDATE server and tolerance window:

1. From the Extensions menu, select RDATE time update.

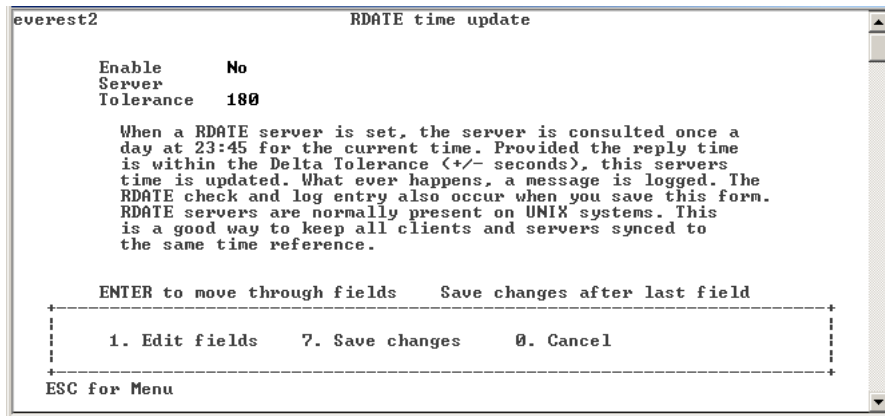


FIGURE A-10 The RDATE Time Update Screen

2. Select 1. Edit fields.
3. Enter the RDATE server name or IP address, and press Enter.
4. Enter the tolerance. If the Sun StorEdge 5310 NAS Appliance server time is different than RDATE server time by less than this number of seconds (+ or -), Sun StorEdge 5310 NAS Appliance server time is synchronized with RDATE server time. This check occurs every day at 11:45 PM. Press Enter.
5. Select 7. Save changes.



# Selecting a Language

To select a language:

1. From the Extensions menu, select Language Selection.

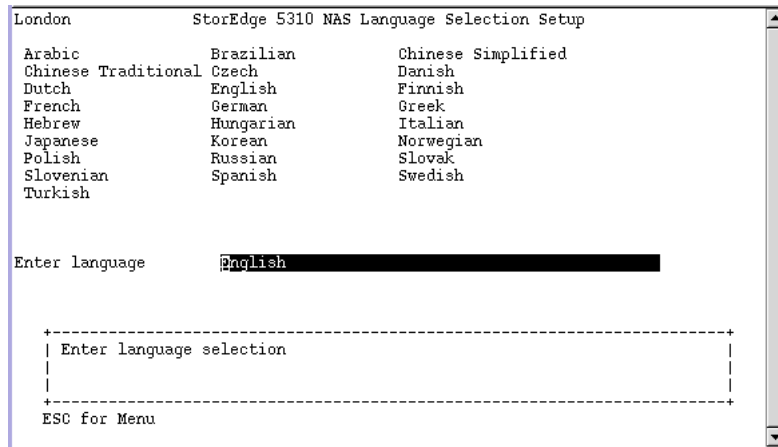


FIGURE A-11 The Language Selection Screen

2. Type the desired language then press Enter. Languages Sun StorEdge 5310 NAS Appliance supports 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.

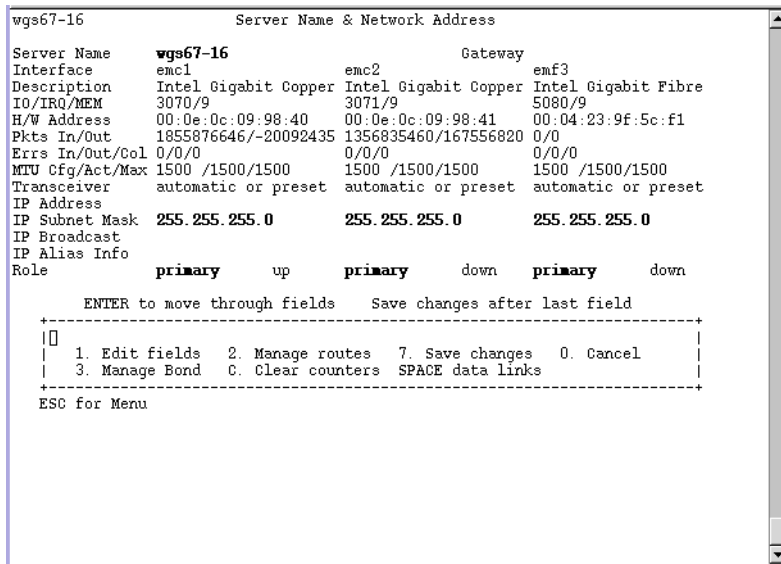


FIGURE A-12 The Host Name and Network Screen

2. Select 2. Manage Routes.

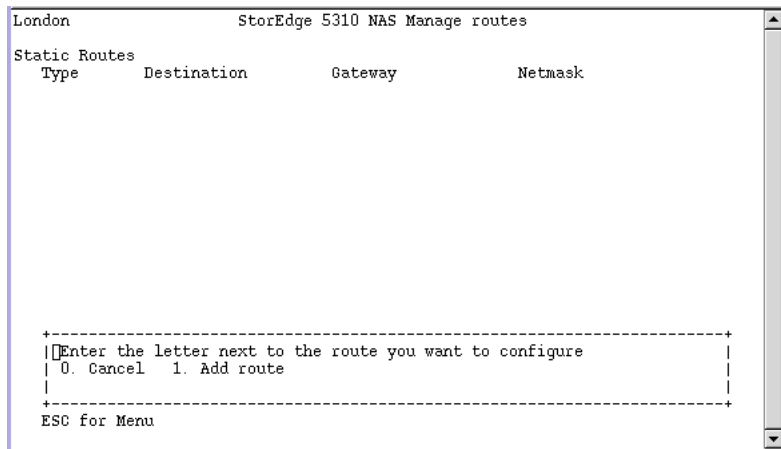
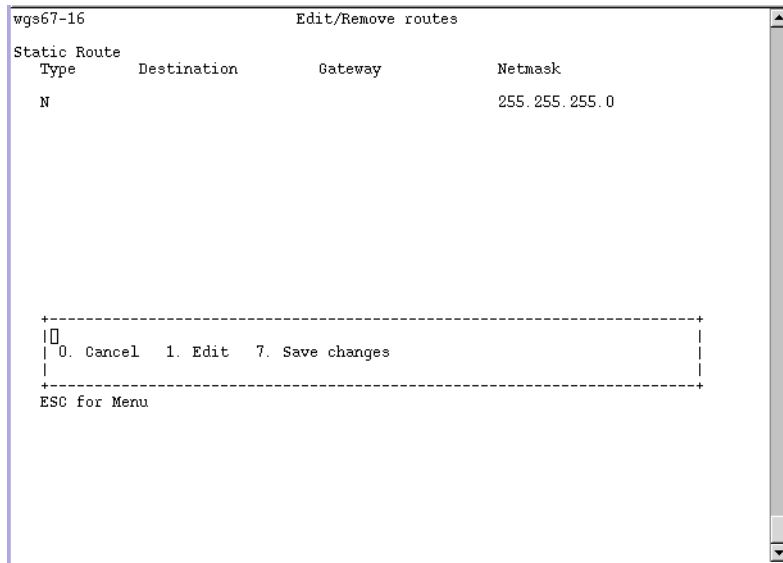


FIGURE A-13 The Manage Routes Screen

**3. Select 1. Add route, then select 1. Edit.**



**FIGURE A-14** The Edit Routes Screen

- 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 StorEdge 5310 NAS Appliance with its destination, then press Enter. The gateway device must connect to the same subnet as the Sun StorEdge 5310 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

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 SYSLOGD UNIX server on the network that can receive the Sun StorEdge 5310 NAS Appliance system log. All of these functions are set up on the same screen.

After SYSLOG 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.

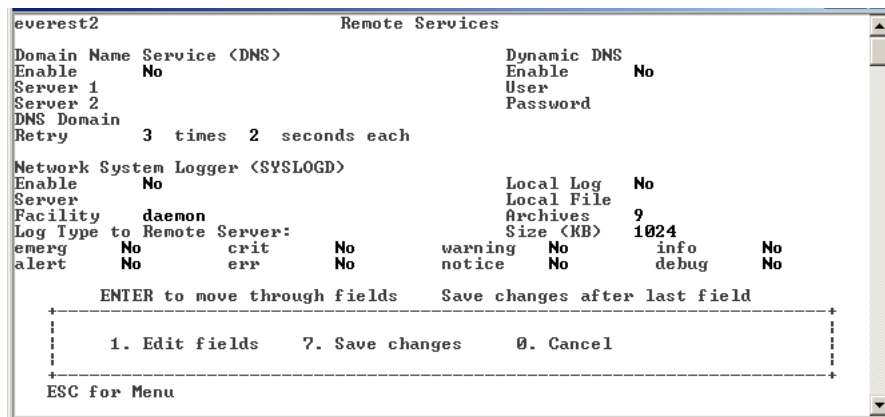


FIGURE A-15 The DNS and SYSLOGD Screen

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. If you do not have a secondary DNS server, leave this field blank. Press Enter.
6. Enter the domain name of the DNS server, then press Enter.
7. Enter the maximum number of times the Sun StorEdge 5310 NAS Appliance 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. This feature lets the Sun StorEdge 5310 NAS Appliance send log messages to a remote SYSLOGD server. If there is no SYSLOGD server on the network, select N. No and skip to step 15.
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 Sun StorEdge 5310 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 non-secure 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. This user must have administrative rights. Press Enter.
  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 filename in the Log File field.
  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+.

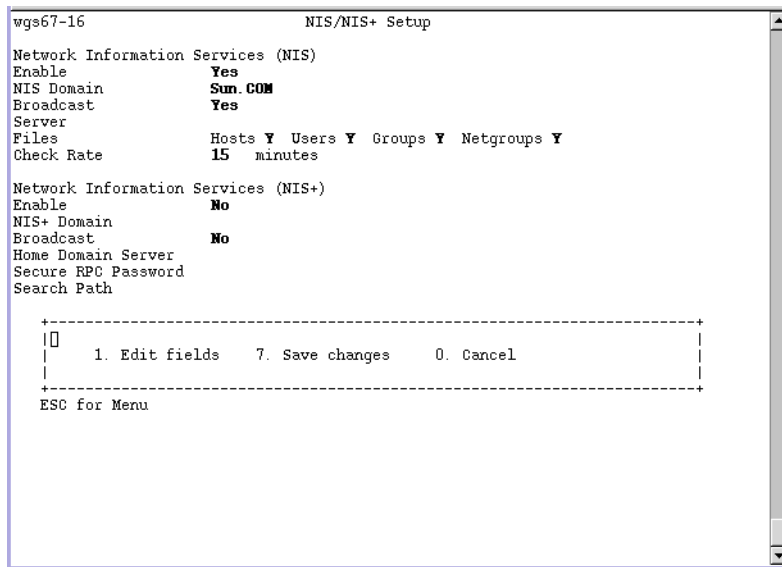


FIGURE A-16 The Configure NIS and NIS+ Screen

2. Select 1. Edit fields.
3. Select Y. Yes to enable the Sun StorEdge 5310 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 StorEdge 5310 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

This menu lets you 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.

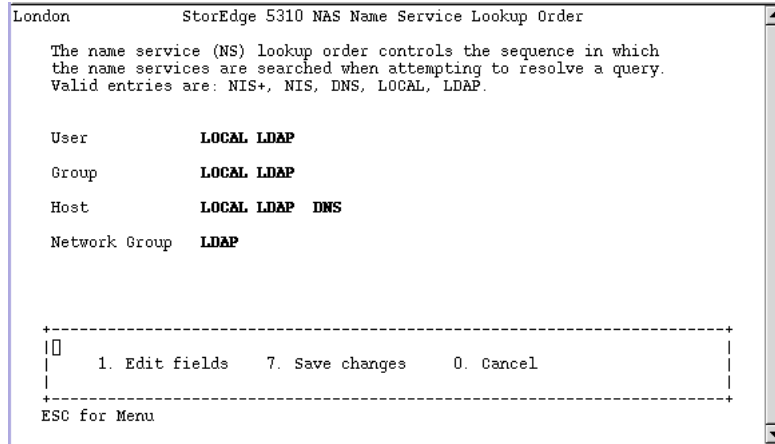


FIGURE A-17 The Lookup Order Screen

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:

- Configuring drive letters
- Configuring a new disk volume
- Verifying a volume
- Renaming a disk partition
- Attaching a segment to a primary volume
- Enabling and disabling quotas and checkpoints
- Deleting a disk volume

## 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.

To manually reassign a drive letter to a file volume:

1. From the Configuration menu, select Drive Letters.

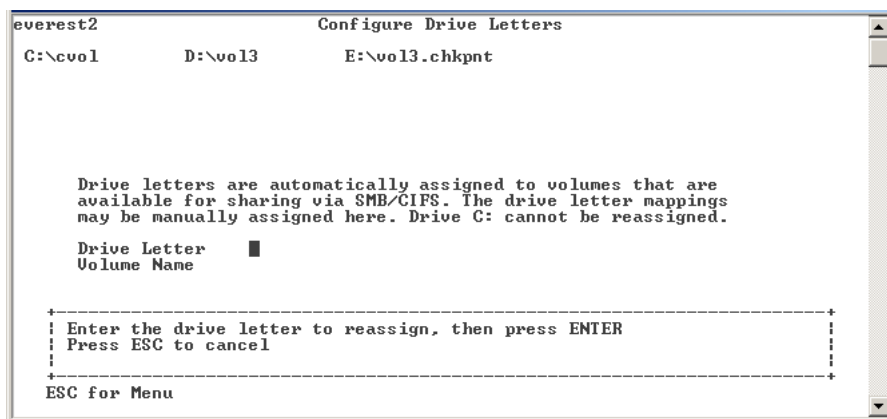


FIGURE A-18 The Drive Letter Assignment Screen

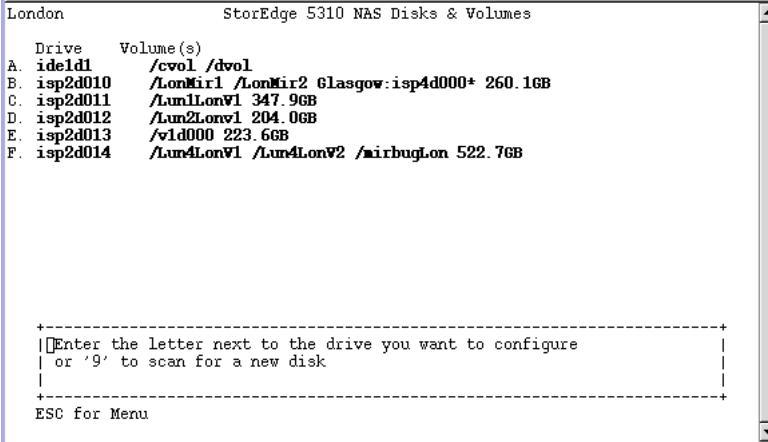
2. Enter the drive letter you want to change, then press Enter.

3. Enter the file volume name you want to assign to the new drive letter, then click Enter. You can only assign existing file volumes to drive letters.
4. Press Esc to exit this screen.

## Creating a New File Volume

To create a new file volume:

1. From the Configuration menu, select Disks & Volumes.



```
London                               StorEdge 5310 NAS Disks & Volumes
Drive   Volume(s)
A. ide1d1 /cvol /dvol
B. isp2d010 /LonMir1 /LonMir2 Glasgow:isp4d000* 260.1GB
C. isp2d011 /Lun1LonV1 347.9GB
D. isp2d012 /Lun2LonV1 204.0GB
E. isp2d013 /v1d000 223.6GB
F. isp2d014 /Lun4LonV1 /Lun4LonV2 /mirbugLon 522.7GB

+-----+
|Enter the letter next to the drive you want to configure
| or '9' to scan for a new disk
|
+-----+
ESC for Menu
```

FIGURE A-19 The Disks and Volumes Screen

2. Enter the letter of the drive you want to configure.

```
London                               StorEdge 5310 NAS Configure Disk
Disk isp2d014   Size MB 697485   SUN   CSM100_R_FC

# START SEC  SIZE SEC  TYPE  C OWNER      USE%  FREE SIZE  REQS ACTIVE
1      240 102400000 sfs2  /Lun4LonV1  34%  32.047G/47.977G  649+0
2 102400240 127270912 sfs2  /Lun4LonV2   1%  59.630G/59.630G  529+0
3 229671152 102400000 sfs2  /mirbugLon   1%  47.977G/47.977G  529+0
4 332071152 1096378765 --    1096378765 sectors (522.7GB) free
5 1428449917      0 --
6 1428449917      0 --
7 1428449917      0 --
8 1428449917      0 --

+-----+
| 1. Edit                                     |
| SPACE page display                         0. Cancel |
+-----+
ESC for Menu
```

FIGURE A-20 The Volume Creation Screen (1)

3. Select 1. Edit.

```
London                               StorEdge 5310 NAS Configure Disk
Disk isp2d014   Size MB 697485   SUN   CSM100_R_FC

# START SEC  SIZE SEC  TYPE  C OWNER      USE%  FREE SIZE  REQS ACTIVE
1      240 102400000 sfs2  /Lun4LonV1  34%  32.047G/47.977G  649+0
2 102400240 127270912 sfs2  /Lun4LonV2   1%  59.630G/59.630G  529+0
3 229671152 102400000 sfs2  /mirbugLon   1%  47.977G/47.977G  529+0
4 332071152 1096378765 --    1096378765 sectors (522.7GB) free
5 1428449917      0 --
6 1428449917      0 --
7 1428449917      0 --
8 1428449917      0 --

+-----+
| 1. Create partition                         |
| Navigation: Up, Dn                         0. Cancel |
+-----+
ESC for Menu
```

FIGURE A-21 The Volume Creation Screen (2)

#### 4. Select 1. Create partition.

```
London                               StorEdge 5310 NAS Configure Disk
Disk isp2d014   Size MB 697485   SUN   CSM100_R_FC

# START SEC  SIZE SEC  TYPE  C OWNER      USE%  FREE SIZE  REQS ACTIVE
1      240 102400000 sfs2  /Lun4LonV1  34%  32.0476/47.9776  651+0
2 102400240 127270912 sfs2  /Lun4LonV2  1%  59.6306/59.6306  531+0
3 229671152 102400000 sfs2  /airbugLon  1%  47.9776/47.9776  531+0
4 332071152 1096378765 -- 1096378765 sectors (522.76E) free
5 1428449917 0 --
6 1428449917 0 --
7 1428449917 0 --
8 1428449917 0 --
Start sec Size Sec Type Name Com Size MB
sfs2 testvol 052144

-----
| Enter a size for this new partition between 8mb and 262144mb.
|
| decimal (0-9) then press ENTER
|
-----
ESC for Menu
```

FIGURE A-22 The Volume Creation Screen (3)

#### 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 you have a license for the Compliance Archiving Software, the system will ask if you want to “Enable Compliance Archiving on this volume?” If you wish to created a compliance-enabled volume, press Y.



---

**Caution** – Once you enable compliance archiving on a volume, that volume cannot be deleted, renamed, or have compliance archiving disabled.

---

#### 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

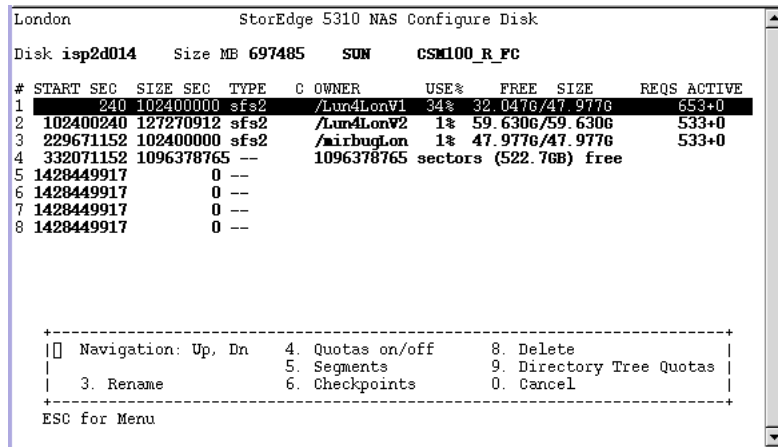
---

**Note** – Compliance-enabled volumes cannot be renamed.

---

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**.



**FIGURE A-23** The Configure Disk Screen

4. Select **3. Rename**.
5. Enter the new name of the partition and press **Enter**.

## 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.

---

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 space bar to scan through them.

---

3. Type the number next to the partition you are changing.

4. Select 5. Segments.

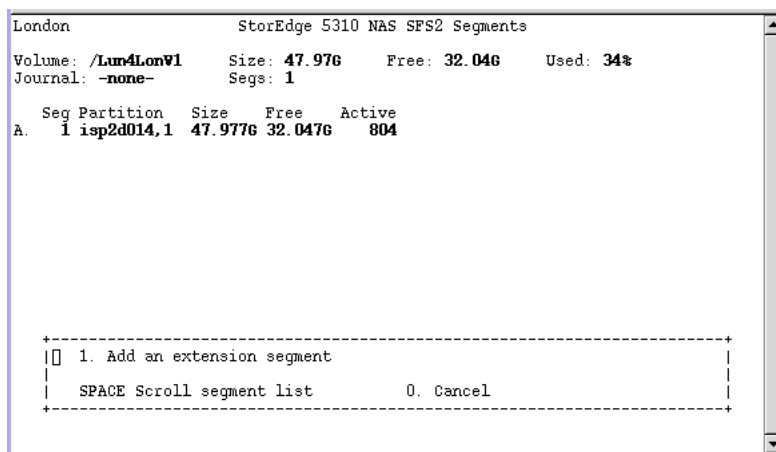


FIGURE A-24 The Segments Screen

5. Select 1. Add an extension segment.

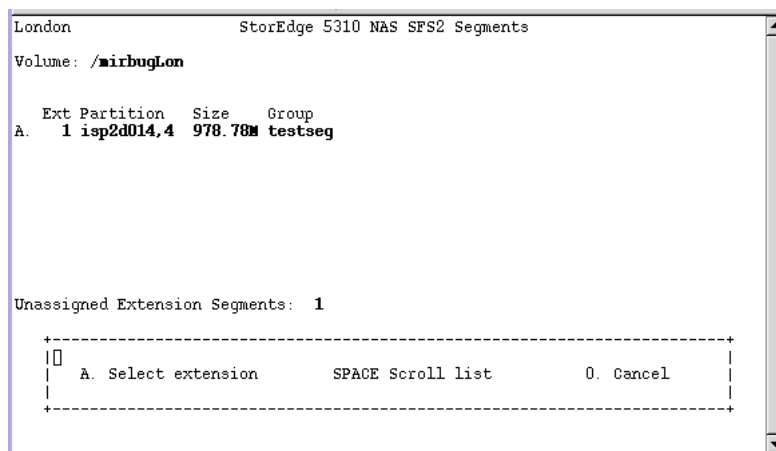


FIGURE A-25 The Add an Extension Segment Screen (1)

6. Select the letter next to the extension drive you want.

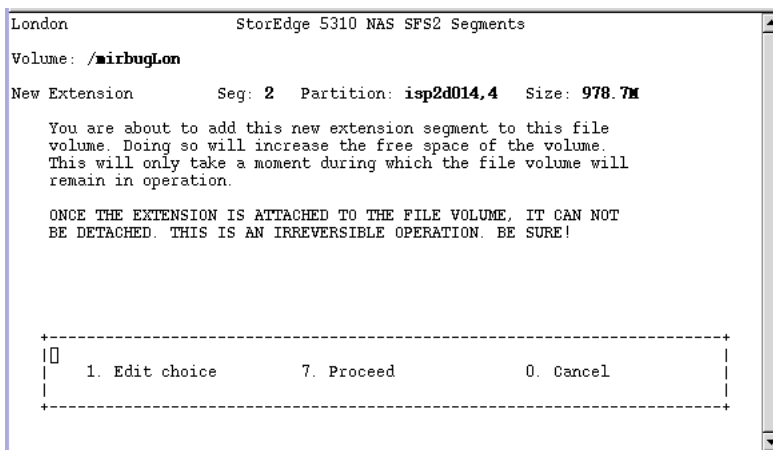


FIGURE A-26 The Add an Extension Segment Screen (2)

7. Select 7. Proceed.

## Deleting a File Volume

---

**Note** – 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 space bar 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.

---

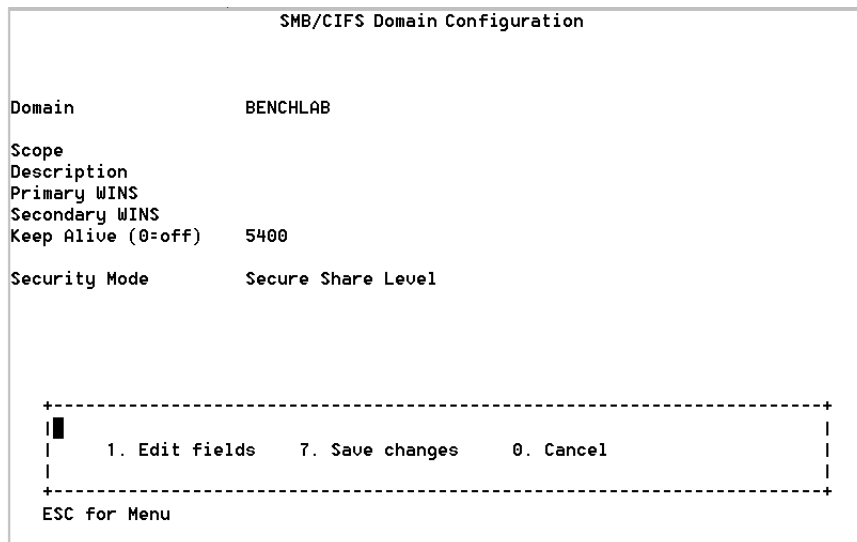
## Shares and Quotas

### 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 StorEdge 5310 NAS Appliance.

#### Setting up Shares

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select A. Domain Configuration.



**FIGURE A-27** The SMB/CIFS Domain Configuration Screen



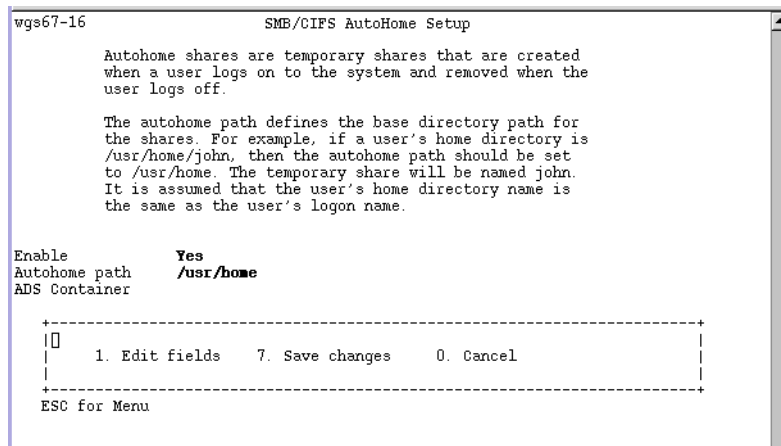
3. Enter a workgroup or domain name in the Domain field.
4. Define the domain Scope, if applicable.
5. Enter a text Description of the Sun StorEdge 5310 NAS Appliance server.
6. Enter the IP address of the primary and secondary Windows Internet Naming Service (WINS) servers, if applicable.
7. Assign 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 StorEdge 5310 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.

To enable autohome shares:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select F. Autohome Setup.



**FIGURE A-28** The SMB/CIFS Autohome Setup Screen

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 to `/usr/home`. The temporary share is named `john`. The Sun StorEdge 5310 NAS Appliance 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 Sun StorEdge 5310 NAS Appliance.

To set up a share:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.

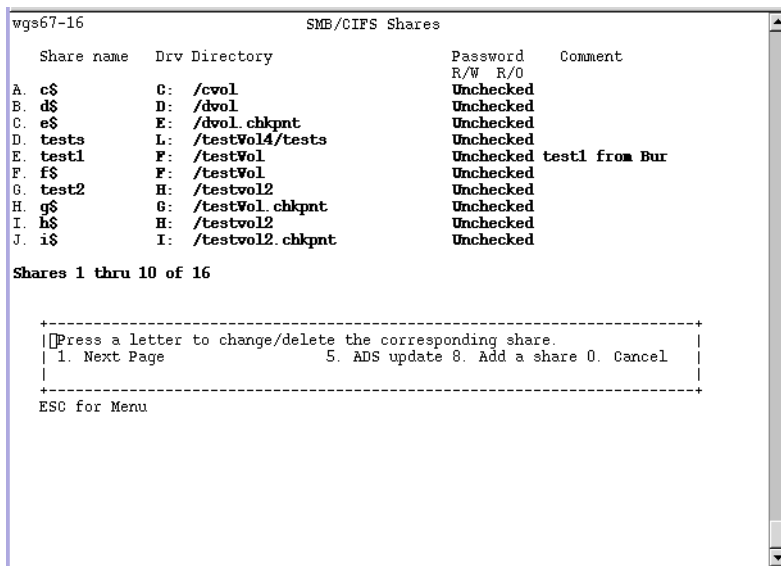


FIGURE A-29 The SMB/CIFS Shares Screen

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 drop-down list, 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. Enter the ADS container, as described in Step 7 of "Adding a Share" on page 232.
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 Services (ADS)

When ADS is enabled and set up on this screen, the Sun StorEdge 5310 NAS Appliance automatically performs ADS updates.

To enable ADS service:

1. From the Extensions menu, select ADS Setup.

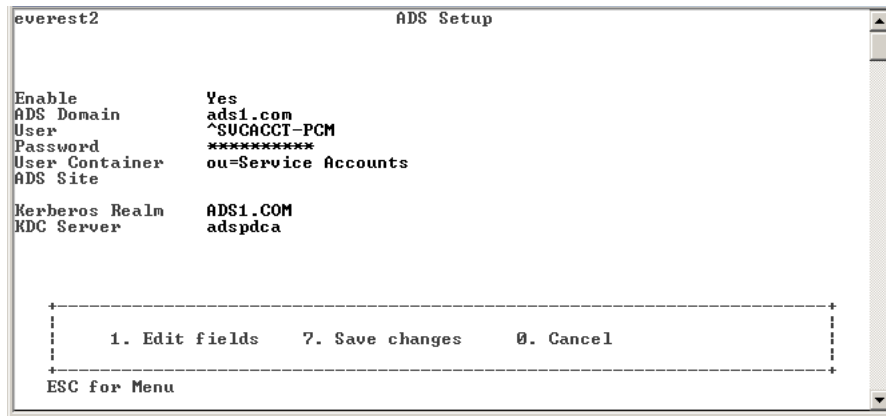


FIGURE A-30 The ADS Setup Screen

2. Select 1. Edit fields.
3. Select Y. Yes to let the ADS client publish Sun StorEdge 5310 NAS Appliance shares to ADS.
4. Enter the Windows domain on which ADS is running. The Sun StorEdge 5310 NAS Appliance must also belong to this domain. Press Enter.
5. Enter the name of a Windows user with administrative rights. The ADS client verifies secure ADS updates with this user. Press Enter.
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 "Setting Up ADS" on page 81.  
Press Enter when you have entered the user container.
8. Enter the name of the local ADS site in the Site field.
9. Enter, in upper-case letters, the Kerberos realm name used to identify ADS. This is normally the ADS domain. Press Enter.

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. Press Enter.
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

### Configuring Sun StorEdge 5310 NAS Appliance User Groups

The requirements for Sun StorEdge 5310 NAS Appliance built-in local groups are different from those of a Windows NT system. For a complete description of user groups, see "Sun StorEdge 5310 NAS Appliance Local Groups" on page 93.

## Adding a Group

To add a group:

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.

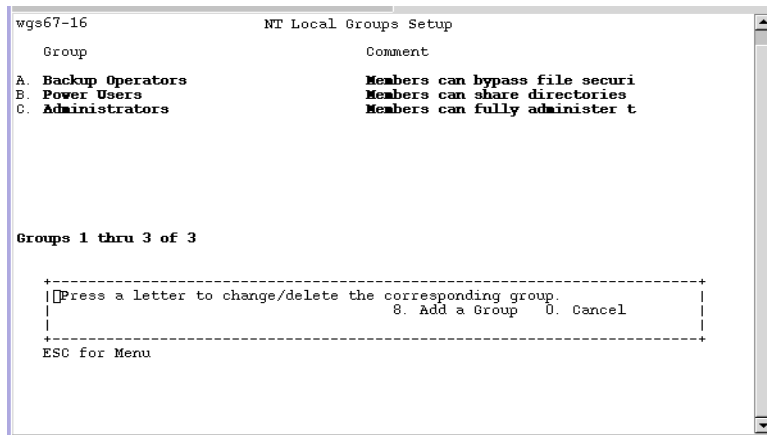


FIGURE A-31 The Local Groups Setup Screen

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 Group Member

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\user name."**  
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 Group Member

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.**

## Group Privileges

A description of the user group privileges is provided in "Configuring Privileges for Sun StorEdge 5310 NAS Appliance Local Groups" on page 94.

## Modifying Local Group Privileges

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.

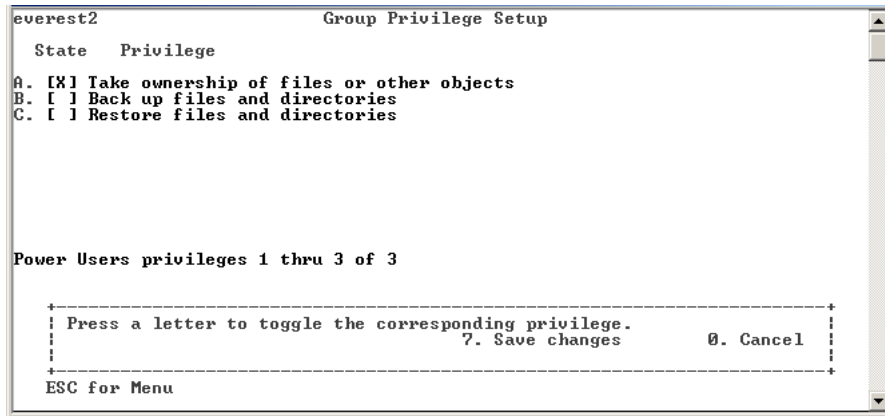


FIGURE A-32 The Modify Group Privileges Screen

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.

---

## Mapping User and Group Credentials

For a complete description of user and group credentials, see "Mapping User and Group Credentials" on page 101.

### Adding a User Map

To add a user map:

1. From the Extensions menu, select CIFS/SMB Configuration.



## 2. Select C. User Mapping.

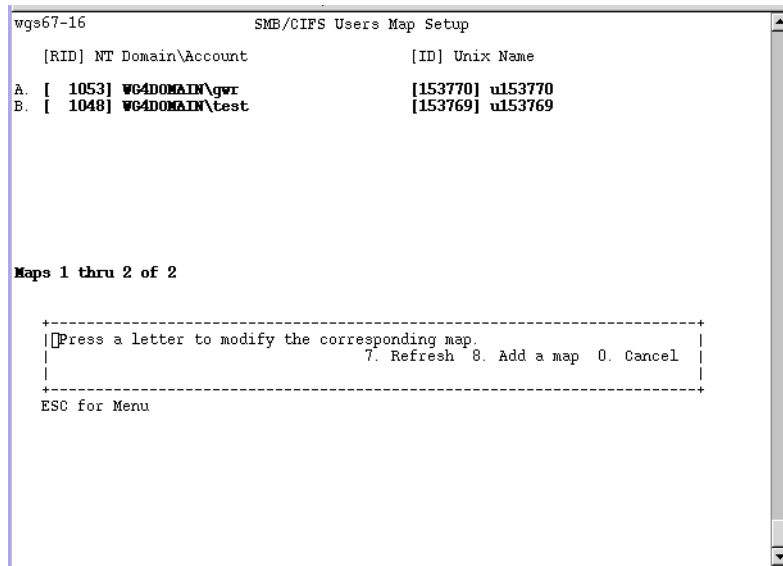


FIGURE A-33 Users Map Setup Screen

## 3. Press 8. Add a map.

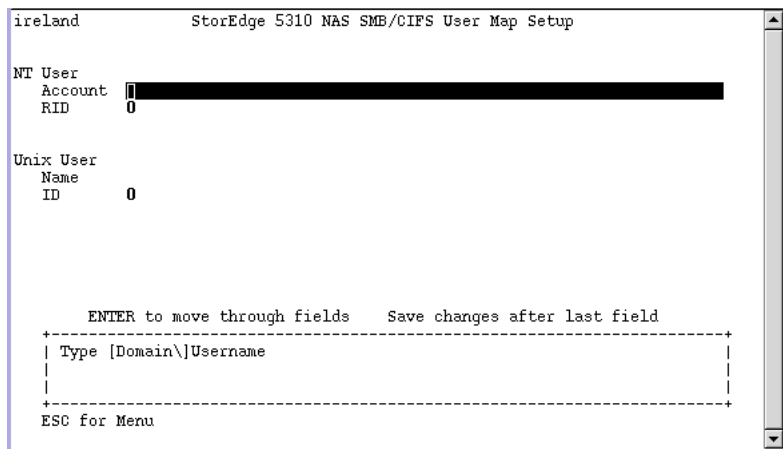


FIGURE A-34 Users Map Setup Screen (2)

## 4. In the Account field, enter the domain and name of the NT user 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 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 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 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.

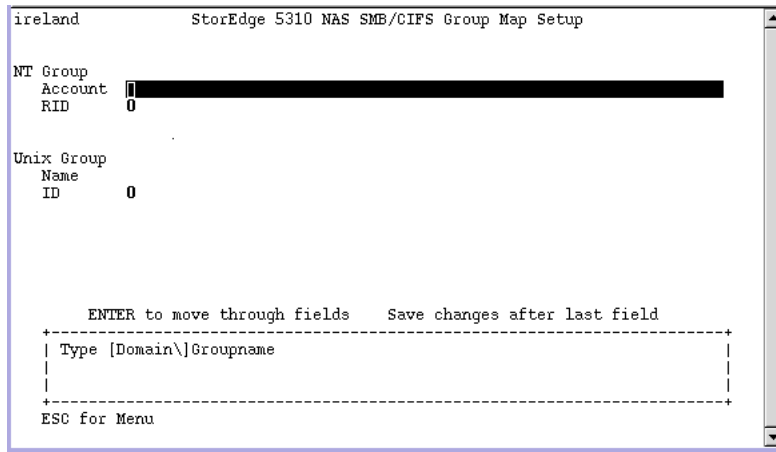


FIGURE A-35 The Group Map Setup Screen

4. In the Account field, enter the domain and name of the NT group 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 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 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 you want to delete.**
  4. **Press 8. Delete.**
- 

## Hosts

### Configuring the Host List

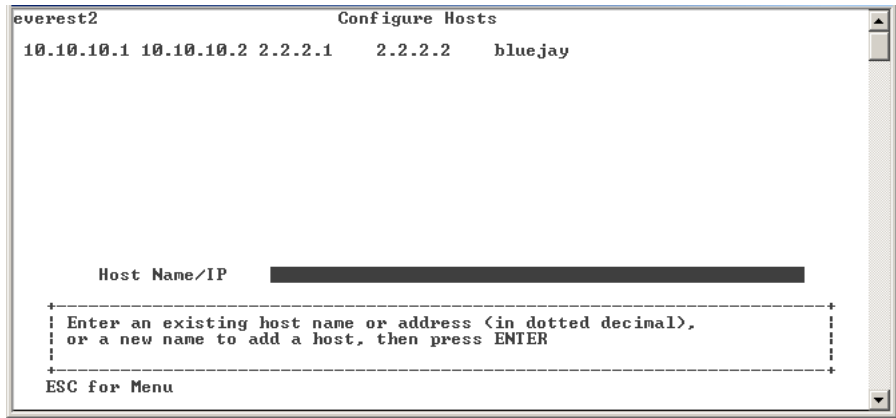
The console allows you to configure host information. From the main menu, select **Hosts** to add, edit, or delete hosts.

### 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.



**FIGURE A-36** The New Host Screen

3. Press Enter to add the host.
4. Enter the new host IP address.
5. Select 7. Save changes.

## Editing a 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.

### Adding a Trusted Host

To designate a trusted host:

1. From the Access Control menu, select Trusted Hosts.

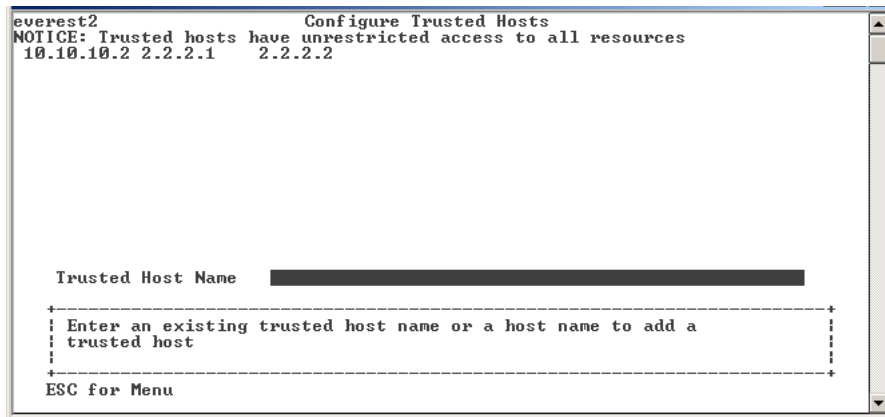


FIGURE A-37 The Trusted Hosts Screen

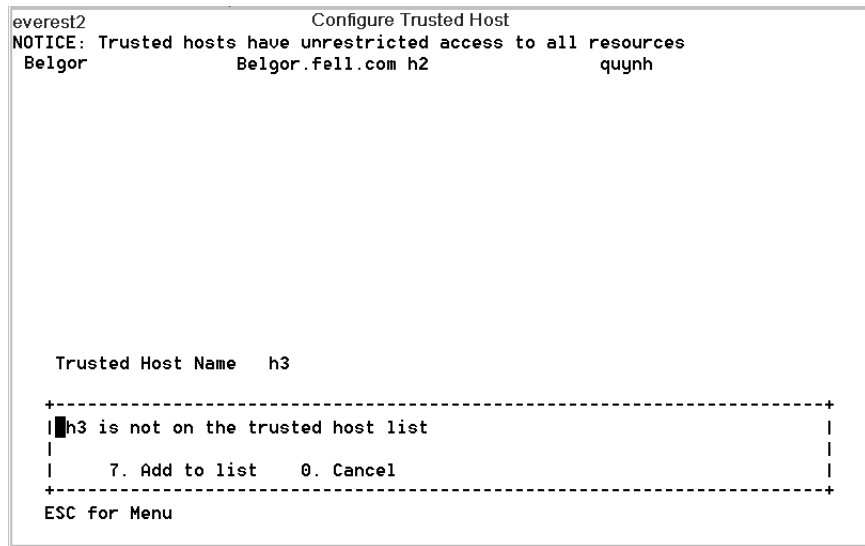
2. Type a new or existing host name, then press Enter.

---

**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.



**FIGURE A-38** The Trusted Host Access Screen

**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 nor write, to the **cvol** volume.

---

**Note** – Trusted hosts are automatically granted read/write access to file volumes regardless of the volumes' access settings.

---

To manage volume access for NFS clients:

1. From the Access Control menu, select Volume Access.

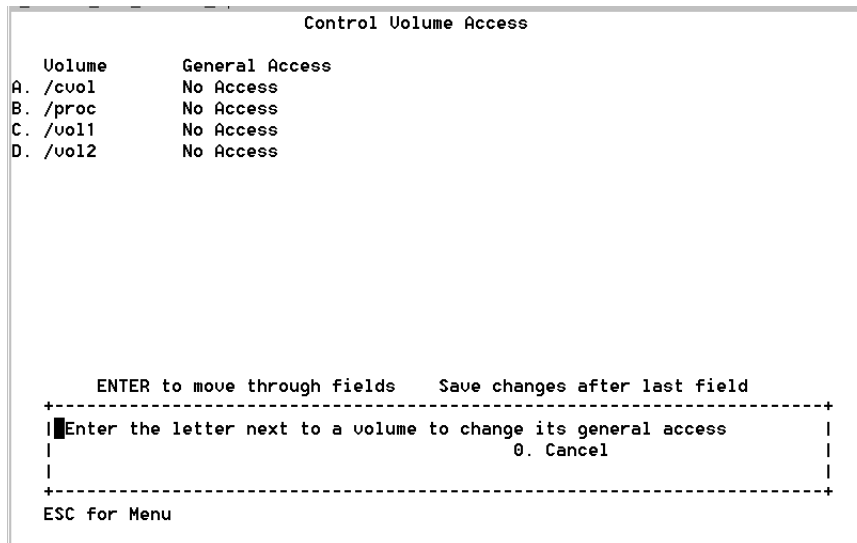


FIGURE A-39 The Volume Access Screen

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

Use the **Lock Console** menu option 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).**

---

## Monitoring

### 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.

```
pamela                               SNMP

Community:                public
Contact Info:             unknown
System Location:         unknown

Trap Destination Table:
  Version  Community      Address          Port    Status

1
2
3
4
5

+-----+
| 1 - 5. Edit a Trap Destination  6. Edit Community |
| 7. Edit Contact  8. Edit Location  0. Exit |
|-----|
ESC for Menu
```

FIGURE A-40 The SNMP Configuration Screen

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 StorEdge 5310 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.

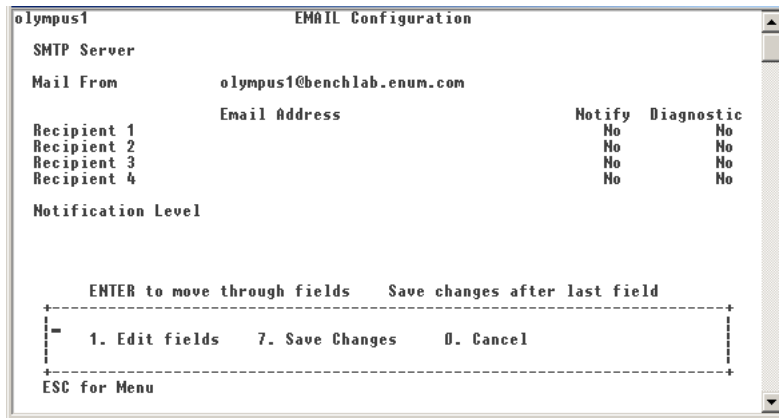


FIGURE A-41 The Email Configuration Screen

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.

---

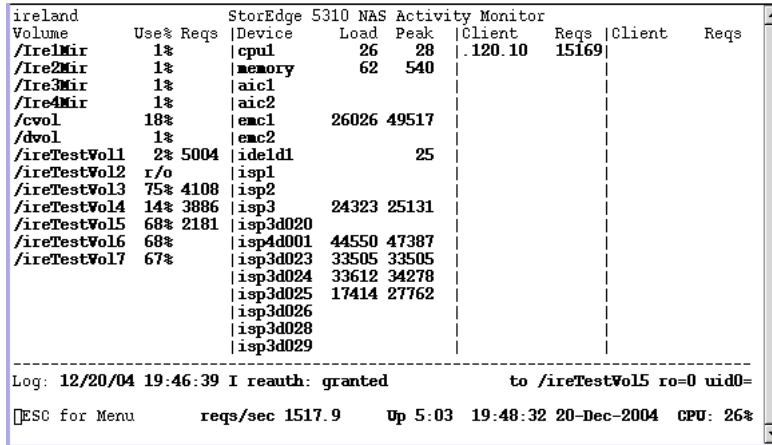
- **Recipient 1..4**—These are the email addresses of the four people automatically notified in case of a problem.
  - **Notification Level**—The level a problem must be at before the recipients are notified through email. Select one of the following:
    - **Errors**—Notifications sent only for errors
    - **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. Select 0. Cancel to cancel the operation.
5. Press Esc to return to the main menu.

# Viewing the Activity Monitor

The activity screen continuously reports the status of your server.

To view the activity monitor:

1. From the Operations menu, choose Activity Monitor.



The screenshot shows a terminal window titled "ireland" displaying the "Activity Monitor" screen. The screen contains a table with columns for Volume, Use%, Reqs, Device, Load, Peak, Client, and Reqs. The data is as follows:

Volume	Use%	Reqs	Device	Load	Peak	Client	Reqs	Client	Reqs
/Ire1Mir	1%		cpu1	26	28	.120.10	15169		
/Ire2Mir	1%		memory	62	540				
/Ire3Mir	1%		aic1						
/Ire4Mir	1%		aic2						
/cvol	18%		emc1	26026	49517				
/dvol	1%		emc2						
/ireTestVol1	2%	5004	ide1d1		25				
/ireTestVol2	r/o		isp1						
/ireTestVol3	75%	4108	isp2						
/ireTestVol4	14%	3886	isp3	24323	25131				
/ireTestVol5	68%	2181	isp3d020						
/ireTestVol6	68%		isp4d001	44550	47387				
/ireTestVol7	67%		isp3d023	33505	33505				
			isp3d024	33612	34278				
			isp3d025	17414	27762				
			isp3d026						
			isp3d028						
			isp3d029						

Log: 12/20/04 19:46:39 I reauth: granted to /ireTestVol5 ro=0 uid0=  
[ESC for Menu reqs/sec 1517.9 Up 5:03 19:48:32 20-Dec-2004 CPU: 26%

FIGURE A-42 The Activity Monitor Screen

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

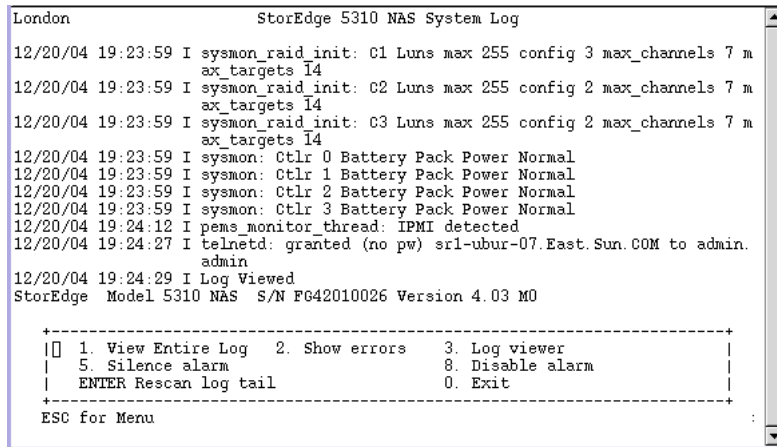
2. Press Esc to return to the main menu.

# Viewing the System Log

Use the **System Log** screen to display the most recent log entries.

To view the system log:

## 1. From the Operations menu, select Show Log.



```
London                               StorEdge 5310 NAS System Log
12/20/04 19:23:59 I sysmon_raid_init: C1 Luns max 255 config 3 max_channels 7 m
ax_targets I4
12/20/04 19:23:59 I sysmon_raid_init: C2 Luns max 255 config 2 max_channels 7 m
ax_targets I4
12/20/04 19:23:59 I sysmon_raid_init: C3 Luns max 255 config 2 max_channels 7 m
ax_targets I4
12/20/04 19:23:59 I sysmon: Ctlr 0 Battery Pack Power Normal
12/20/04 19:23:59 I sysmon: Ctlr 1 Battery Pack Power Normal
12/20/04 19:23:59 I sysmon: Ctlr 2 Battery Pack Power Normal
12/20/04 19:23:59 I sysmon: Ctlr 3 Battery Pack Power Normal
12/20/04 19:24:12 I pems_monitor_thread: IPMI detected
12/20/04 19:24:27 I telnetd: granted (no pw) srl-ubur-07.East.Sun.COM to admin.
admin
12/20/04 19:24:29 I Log Viewed
StorEdge Model 5310 NAS S/N F642010026 Version 4.03 M0

+-----+
| 1. View Entire Log  2. Show errors  3. Log viewer
| 4. Silence alarm    5. Disable alarm
| ENTER Rescan log tail 6. Exit
+-----+
ESC for Menu
```

**FIGURE A-43** The System Log Screen

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

You can view port bond information in the **Host Name & Network** screen.

1. From the Configuration menu, select **Host Name & Network**.

```
wgs67-16          Server Name & Network Address
Server Name      wgs67-16          Gateway
Interface        emc1          emc2          emf3
Description      Intel Gigabit Copper Intel Gigabit Copper Intel Gigabit Fibre
IO/IRQ/MEM       3070/9       3071/9       5080/9
H/W Address      00:0e:0c:09:98:40 00:0e:0c:09:98:41 00:04:23:9f:5c:f1
Pkts In/Out      1855876646/-20092435 1356835460/167556820 0/0
Errs In/Out/Col  0/0/0        0/0/0        0/0/0
MTU Cfg/Act/Max  1500 /1500/1500 1500 /1500/1500 1500 /1500/1500
Transceiver      automatic or preset automatic or preset automatic or preset
IP Address
IP Subnet Mask   255.255.255.0   255.255.255.0   255.255.255.0
IP Broadcast
IP Alias Info
Role             primary        up             primary        down           primary        down
ENTER to move through fields   Save changes after last field
+-----+
| 1. Edit fields  2. Manage routes  7. Save changes  0. Cancel      |
| 3. Manage Bond  C. Clear counters SPACE data links |
+-----+
ESC for Menu
```

FIGURE A-44 Viewing Port Bonding Information (page 1)

2. Press the spacebar to scroll to the next page.

```
wgs67-16          Server Name & Network Address
Server Name      wgs67-16          Gateway
Interface        bond1/PA
Description      Channel Bonding
IO/IRQ/MEM       1/0
H/W Address      00:0e:0c:09:98:40
Pkts In/Out      -1581965526/-9500845
Errs In/Out/Col  0/0/0
MTU Cfg/Act/Max  1500 /1500/1500
Transceiver      automatic or preset
IP Address
IP Subnet Mask   255.255.255.0
IP Broadcast
IP Alias Info
Role             primary        down
ENTER to move through fields   Save changes after last field
+-----+
| 1. Edit fields  2. Manage routes  7. Save changes  0. Cancel      |
| 3. Manage Bond  C. Clear counters SPACE data links |
+-----+
ESC for Menu
```

FIGURE A-45 Viewing Port Bonding Information (page 2)

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

The checkpoint analysis shows the days and times that all checkpoints are created and removed.

To view the checkpoint analysis:

1. From the Configuration menu, select Disks & Volumes.
2. Type the letter corresponding to the drive you are configuring.
3. Select Change/Delete <volume name>.
4. Select 6. Checkpoints.
5. Select 3. Analysis. Scroll through the analysis using the spacebar.

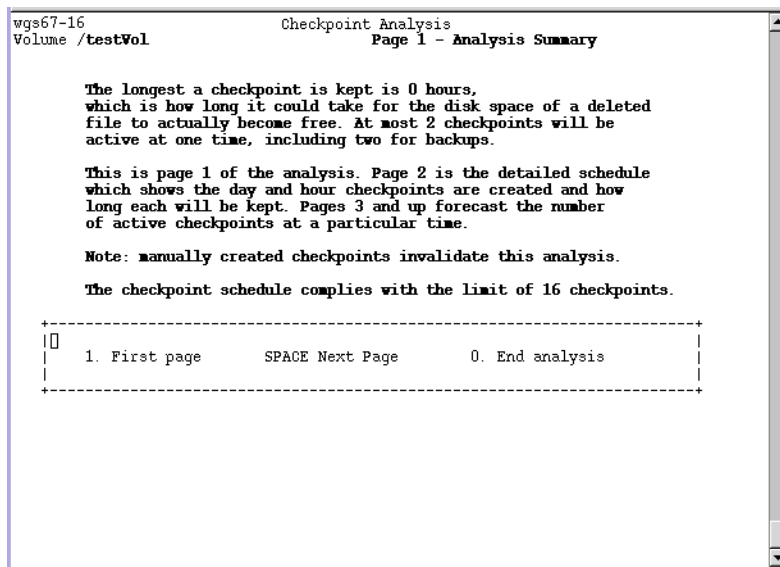


FIGURE A-46 Checkpoint Analysis

6. Select 0. End Analysis to exit this screen.

---

# System Maintenance

## 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.

You can set up three types of users:

- **Administrators** who have the username “admin” and use the same password used by GUI clients.

The administrator has “root” access to all volumes, directories, and files on the Sun StorEdge 5310 NAS Appliance. The administrator’s home directory is defined as “/”.

- **Users** who have a username and a password specified in the local password file or on a remote NIS or NIS+ name server.

The user has access to all 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 login with the username “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 setup FTP access:

1. **From the Extensions menu, select FTP Configuration.**



## 2. Select 1. Edit Fields.

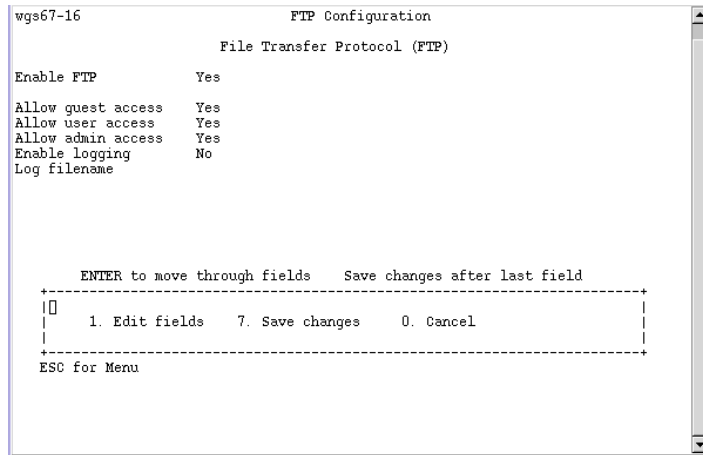


FIGURE A-47 FTP Configuration

## 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 StorEdge 5310 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 StorEdge 5310 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.

# Shutting Down the System

The Sun StorEdge 5310 NAS Appliance system is designed for continuous operation.

To shut down the system:

## 1. From the Operations menu, select Shutdown.

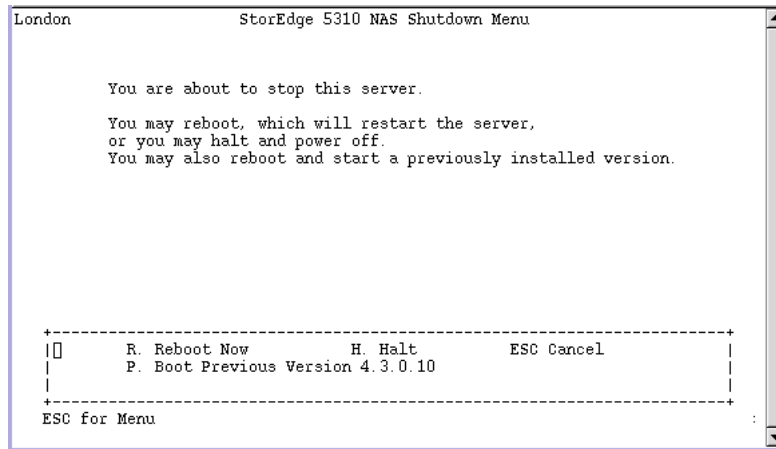


FIGURE A-48 The Shutdown Menu Screen

## 2. Select the desired option by typing the appropriated 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 versions 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 Failover

The **Failover** menu manages disk resources when a recoverable RAID error occurs. Failover occurs when one of the two RAID controllers or heads becomes unreliable and all LUNs under its control must be moved to the stable controller or head.



# Configuring Failback

To restore (*recover*) to the preferred (*new*) configuration:

1. **Replace or repair the faulty component and make sure it is online.**
2. **From the Extensions menu, select Failover/Move LUNs.**
3. **Select 1. Restore.**
4. **Select Y. Yes to proceed with the restore process.**

# Configuring LUN Paths

See "About LUN Paths" on page 19 for more information on the subject and the use of the GUI in setting the LUN paths.

To set or 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 filesystems on that LUN. On a Sun StorEdge 5310 Cluster system, only the head that "owns" a LUN can reassign it to another head.

---

**Note** – On a Sun StorEdge 5310 Cluster system, 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.

---



4. Type the number of the desired LUN path to which you want to change and press Enter.

Evenly divide 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

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 space bar to scan through them.

---

3. Select 1. Edit.

```

London                               StorEdge 5310 NAS Configure Disk
Disk isp4d004   Size MB 697485   SUN   CSM100_R_PC

# START SEC  SIZE SEC  TYPE  C OWNER      USE%   FREE  SIZE  REQS ACTIVE
1  240 102400000  sfs2  /Lun4LonV1  34%  32.047G/47.977G  438*5
2  102400240 127270912  sfs2  /Lun4LonV2  1%  59.630G/59.630G  35*0
3  229671152 102400000  sfs2  /mirbugLon  1%  47.977G/47.977G  35*0
4  332071152  2048000  sfs2ext ~testseg  978M
5  334119152 1094330765 --      1094330765 sectors (521.8GB) free
6  1428449917 0 --
7  1428449917 0 --
8  1428449917 0 --

+-----+
|[] Navigation: Up, Dn  4. Quotas on/off      8. Delete      |
| 3. Rename            5. Segments        9. Directory Tree Quotas |
| 6. Checkpoints       0. Cancel              |
+-----+
ESC for Menu
  
```

FIGURE A-52 The Configure Disk Screen

#### 4. Select 6. Checkpoints.

```
London          StorEdge 5310 NAS Checkpoint Configuration
Volume /Lun4LonV1  Enable Checkpoints      Yes  Use for Backups Yes
Status 0/16 checkpoints, 4K bytes used

Pseudo Vol    /Lun4LonV1.chkpt

Automatic      Yes
  Enable Description  Days    Hours AM    Hours PM    Keep
                  SMTWTFS  M1234567890E N1234567890E Days+Hours
1. No
2. No
3. No
4. No
5. No

+-----+
|  | 1. Edit   3. Analysis  7. Save Changes  0. Cancel
|  |          |           |           |           |  ?  Help
|  |          |           |           |           |
+-----+
```

FIGURE A-53 The Checkpoint Configuration Screen

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 the Compliance Archiving Software

If you have purchased, activated, and enabled the Compliance Archiving Software option (see "Sun StorEdge 5310 NAS Appliance Options" on page 133), there are additional settings you can establish using the command line interface.



---

**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 Command Line Interface" on page 205.
2. At the command line enter `fsctl compliance <volume> drt <time>`  
where *<volume>* is the name of the volume you want to set the default retention time on 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 will only support data retention requests from NFS clients. 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 Command Line Interface" on page 205.
2. At the command line enter `fsctl compliance wte on`



## Sun StorEdge 5310 NAS Appliance Error Messages

---

This appendix details the specific error messages sent through email, SNMP notification, the LCD panel, and the system log to notify the administrator in the event of a system error. *SysMon*, the monitoring thread in the Sun StorEdge 5310 NAS Appliance, monitors the status of RAID devices, UPSs, file systems, head units, enclosure subsystems, and environmental variables. Monitoring and error messages vary depending on model and configuration.

In the tables in this appendix, table columns with no entries have been deleted.

---

### About SysMon Error Notification

*SysMon*, the monitoring thread in the Sun StorEdge 5310 NAS Appliance, captures events generated as a result of subsystem errors. It then takes the appropriate action of sending an email, notifying the SNMP server, displaying the error on the LCD panel, writing an error message to the system log, or some combination of these actions. E-mail notification and the system log include the time of the event.

---

## Sun StorEdge 5310 NAS Appliance Error Messages

The following sections show error messages for the Sun StorEdge 5310 NAS Appliance UPS, RAID devices, file system usage, and the IPMI.

# UPS Subsystem Errors

Refer to Table B-1 for descriptions of UPS error conditions.

**TABLE B-1** UPS Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Power Failure	<b>AC Power Failure:</b> 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	<b>AC power restored:</b> AC power restored. System is running on AC power. Severity = Notice	EnvUpsOff Battery	U21 power restored	UPS: AC power restored.
Low Battery	<b>UPS battery low:</b> 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	<b>UPS battery recharged:</b> The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.
Replace Battery	<b>Replace UPS Battery:</b> 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	<b>UPS abnormal temperature/humidity:</b> 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.

**TABLE B-1** UPS Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Write-back cache is disabled.	<p><b>Controller Cache Disabled:</b>                      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</p>		Cache Disabled	write-back cache for ctrl x disabled
Write-back cache is enabled.	<p><b>Controller Cache Enabled:</b>                      System AC power and UPS are reliable again. Write-back cache is enabled.                      Severity = Notice</p>		Cache Enabled	write-back cache for ctrl n enabled
The UPS is shutting down.	<p><b>UPS shutdown:</b>                      The system is being shut down because there is no AC power and the UPS battery is depleted.                      Severity = Critical</p>			UPS: Shutting down
UPS Failure	<p><b>UPS failure:</b>                      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</p>	EnvUpsFail	U25 UPS failure	UPS: Communication failure.

## File System Errors

File system error messages occur when the file system usage exceeds a defined usage threshold. The default usage threshold is 95%.

**TABLE B-2** File System Errors

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
File System Full	<p><b>File system full:</b> File system &lt;name&gt; 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)</p>	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is xx%.

## RAID Subsystem Errors

Table B-3 displays events and error messages for the Sun StorEdge 5310 NAS Appliance.

**TABLE B-3** RAID Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
LUN Failure	<p><b>RAID LUN failure:</b> RAID LUN <i>N</i> failed and was taken offline. Slot <i>n</i> is offline. Action: Replace bad drives and restore data from backup. Severity = Error</p>	RaidLunFail	R10 Lun failure	RAID LUN <i>N</i> failed and was taken offline. Slot <i>n</i> is offline. (Severity=Error)
Disk Failure	<p><b>Disk drive failure:</b> Disk drive failure. Failed drives are: Slot#, Vendor, Product ID, Size Severity = Error</p>	RaidDiskFail	R11 Drive failure	Disk drive failure. Failed drives are: Slot#, Vendor, Product ID, Size (Severity=Error)
Controller Failure	<p><b>RAID controller failure:</b> RAID controller <i>N</i> has failed. Action: Contact technical support. Severity = Error</p>	RaidController Fail	R12 Ctlr failure	RAID controller <i>N</i> failed.

## IPMI Events

Sun StorEdge 5310 NAS Appliance employs the IPMI board to monitor environmental systems and to send messages regarding power supply and temperature anomalies.

---

**Note** – Device locations are shown in the *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide*.

---

Table B-4 describes the IPMI error messages for the Sun StorEdge 5310 NAS Appliance.

**TABLE B-4** IPMI Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Fan Error	<p><b>Fan Failure:</b> 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</p>	envFanFail trap	P11 Fan xx failed	Blower fan xx has failed!
Power Supply Module Failure	<p><b>Power supply failure:</b> The power supply unit xx has failed. Action: The power supply unit must be replaced as soon as possible. Severity = Error</p>	envPowerFail trap	P12 Power xx failed	Power supply unit xx has failed.
Power Supply Module Temperature	<p><b>Power supply temperature critical:</b> The power supply unit xx is overheating. Action: Replace the power supply to avoid any permanent damage. Severity = Critical</p>	envPowerTemp Critical trap	P22 Power xx overheated	Power supply unit xx is overheating.
Temperature Error	<p><b>Temperature critical:</b> 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</p>	envTemperature Error trap	P51 Temp error	The temperature is critical.

**TABLE B-4** IPMI Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Primary Power Cord Failure	<p><b>Power cord failure:</b> The primary power cord has failed or been disconnected.</p> <p>Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord.</p> <p>Severity = Error</p>	envPrimary PowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
Secondary Power Cord Failure	<p><b>Power cord failure:</b> The secondary power cord has failed or been disconnected.</p> <p>Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord.</p> <p>Severity = Error</p>	envSecondary PowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

# Compliance Archiving Software API

---

The Sun StorEdge 5310 NAS Appliance product supports compliance data storage as a license key enabled software extension called 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.

---

**Note** – Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorEdge 5310 NAS Appliance system hardware. In particular, the Sun StorEdge 5300 RAID EU controller 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 EU 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 StorEdge 5310 NAS Appliance system. Software-controlled data retention can be no stronger than the physical safeguards used to control access to the system's hardware.

---

This appendix is a technical overview of the features and programming interface for the Compliance Archiving Software.

---

# Compliance Features

The Compliance Archiving Software provides storage-level guarantees regarding the accuracy, integrity, and retention of files. This functionality consists of the following three major features:

- WORM (Write-Once, Read-Many) Files
- Per-File Retention Periods
- Administrative Lock-Down

## 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, non-erasable storage, it would be more accurate to call them "permanently read-only." The Sun StorEdge 5310 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 StorEdge 5310 NAS Appliance (NFS and CIFS). In particular, the Sun StorEdge 5310 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 since 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 StorEdge 5310 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—the setuid bit and no other permission bits. 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:

- 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
<b>UNIX</b>	<ul style="list-style-type: none"><li>• Set or clear read permission bits</li><li>• Change file and group owner</li></ul>	<ul style="list-style-type: none"><li>• Enable write and execute bits</li><li>• Clear setuid bit</li><li>• Modify size or modification time (mtime)</li></ul>
<b>Windows</b>	<ul style="list-style-type: none"><li>• Set or clear read permission bits</li><li>• Change archive bit</li><li>• Create and modify Access Control Lists (although a WORM file can never be modified regardless of ACL settings)</li></ul>	<ul style="list-style-type: none"><li>• Change the read-only, system, or hidden bits</li><li>• Modify size or modification time (mtime)</li></ul>

## 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 standard 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 via 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 StorEdge 5310 NAS Appliance share. System calls not listed here behave as normal.

It is important to remember that the interfaces to the Sun StorEdge 5310 NAS Appliance are the NFS and CIFS file access protocols. Thus, this section incorporates both the compliance-related behavior of the Sun StorEdge 5310 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 OS clients and should be the same on other UNIX clients.

## access(2)

Any check for write permission on a WORM file (i.e., 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 (`EACCESS`).

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)`, below).

## read(2), readv(2)

Clients can read WORM files. Since 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 StorEdge 5310 NAS Appliance secure clock, is later than the date stored in the file's `atime` attribute (i.e., 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 (i.e., 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

## 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

### 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.



## Anti-virus 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, including Java, Perl, C++, et al. All of these languages rely on the same underlying system calls to access shares mounted via NFS or CIFS.



## Technical Support and Q&A

---

This appendix provides instructions for sending a diagnostic email and contacting the Sun Microsystems Technical Support team.

If you have problems with the physical components of the Sun StorEdge 5310 NAS Appliance, see the *Sun StorEdge 5310 NAS Appliance Hardware Installation, Configuration, and User Guide*.


---

### Sending a Diagnostic Email Message

The diagnostic email feature allows you to send email messages to the Sun Microsystems Technical Support team or any other desired recipient. Diagnostic e-mail messages include information about the Sun StorEdge 5310 NAS Appliance system configuration, disk subsystem, file system, network configuration, SMB shares, backup/restore processes, /etc information, system log, environment data, and administrator information.

Every diagnostic email message sent includes all of this information, regardless of the problem.

To set up diagnostic email:

1. In the toolbar at the top of the screen, select the  button.

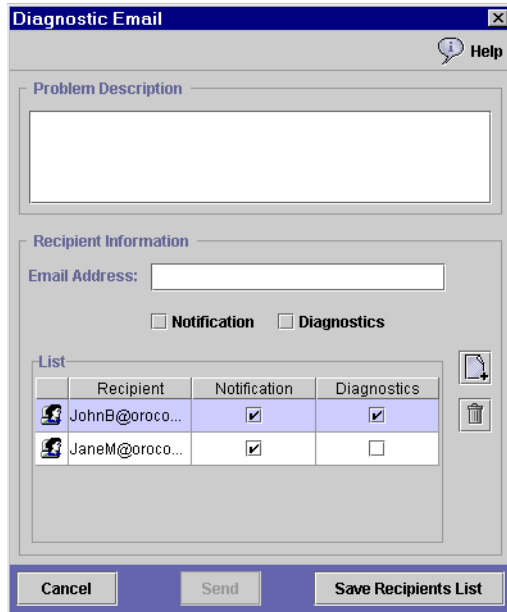


FIGURE D-1 The Diagnostic Email Dialog Box

2. Enter 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 checked for at least one email recipient. If you need to add or make changes to recipients, refer to the instructions in "Setting Up Email Notification" on page 41.
4. Click Send to send the message.

---

## Contacting Technical Support

We hope the instructions provided in this user's guide are complete and clear enough to meet your needs. If you need further assistance, contact Sun Microsystems.

We take pride in providing highly responsive, world-class service to ensure the highest levels of on-going customer satisfaction with all of our products.

For technical problems requiring on-site service, Sun Microsystems provides professional, experienced field engineers, who work closely with our Technical Support Engineers for total solution support. For more information about purchasing an on-site service package for your system, contact your sales representative or reseller.

You can contact Sun Microsystems Technical Support Engineers in a variety of ways or obtain technical information (specifications, files, answers to frequently asked questions) by going to <http://www.sun.com/service/contacting/solution.html>.



# Glossary

---

<b>10Base-T</b>	The IEEE 802.3 standard for Ethernet running over unshielded twisted pair wire.
<b>100Base-TX</b>	The IEEE 802.3 standard for Ethernet running over the same wiring (Category 3, 4, or 5 UTP or STP), but ten times faster than its ancestor, 10BASE-T.
<b>Access Control</b>	Limits user access to resources on a computer network, most commonly by requiring a user name and password. Usually a single logon is sufficient to <i>authenticate</i> , or <i>verify</i> , a user.
<b>Access Rights</b>	Permissions granted to user accounts to allow access to such system resources as file systems, applications, and directories. For example, <i>read-only</i> access allows a user to open or list a file without being able to make changes to the file. Users who are granted access rights to a directory usually have the same access rights to all subdirectories.
<b>Action Button</b>	An action button is a type of interface control that allows you to take an action. When you click the button, the action occurs.
<b>Active/Active Cluster</b>	A pair of identical high availability servers that offer NAS services to client communities. In the event of a failure, the surviving server takes on the services and client community of its failed peer.
<b>Address</b>	See also <i>IP address</i> . An address is also known as location or URL in the Internet world.
<b>Admin</b>	Refers to administrative access to the command interpreter and menus. Admin access gives complete control over server operation and configuration.
<b>ADS</b>	Short for Active Directory Service. ADS is a Windows 2000 namespace that is integrated with the Domain Name System (DNS). ADS stores domain information such as users, groups, and shared resources and makes that information available to Active Directory clients.
<b>Alias IP Address</b>	Multiple IP addresses assigned to a single port, in addition to the primary IP address. All IP aliases for a port must be on the same physical network and share the same netmask and broadcast address as the first or primary IP address. See "About Alias IP Addresses" on page 64.

<b>Alternate Gateway</b>	A network server configured to function as a gateway if the primary gateway server is unavailable.
<b>Autohome Shares</b>	Temporary SMB/CIFS shares that are created when a user logs on to the system and removed when the user logs off. See "About Autohome Shares" on page 117.
<b>Authentication</b>	The process of validating that the user attempting to logon is truly the owner of the account.
<b>BIOS</b>	Stands for basic input/output system. Built-in software that determines what a computer can do without accessing programs from disk.
<b>Boot Up</b>	The process of starting a computer. Booting up involves checking all hardware components, initializing system components, and loading the operating system.
<b>Broadcast Address</b>	The IP address used to send broadcast messages to the subnet. A broadcast message is sent to all nodes on the network.
<b>Browser</b>	Software used for access to information on the World Wide Web. Microsoft Internet Explorer and Netscape Navigator are examples of browsers. See also <i>Web Browser</i> .
<b>CIFS</b>	Stands for Common Internet File System. An enhanced version of the SMB file-sharing protocol that allows groups of users to work together and share documents over the Internet in the same way as in local area networks. The major features of CIFS include: <ul style="list-style-type: none"> <li>■The same multi-user read and write operations, locking, file sharing syntax, and SMB.</li> <li>■Use of TCP/IP and DNS (Domain Name System).</li> <li>■Support of multiple client access and updates of the same file without conflicts.</li> <li>■Fault tolerant operation that reopens connections and reopens files that were open prior to interruption.</li> <li>■Security features that support both anonymous transfers and secure authenticated access to named files.</li> </ul> File and directory security policies are easy to administer and use the same share-level and user-level security policies that are used in Windows.
<b>Cluster</b>	A pair of identical NAS servers providing redundant high availability NAS services via failover protection.
<b>Compliance</b>	A reference to the Compliance Archiving Software option that enables compliance archiving with the stringent data management and retention requirements of the Securities and Exchange Commission (SEC 240.17a-4)



<b>Configuration</b>	(1) The manner in which the software and hardware of an information processing system are organized and interconnected. (2) The physical and logical arrangement of programs and devices that make up a data processing system. (3) The devices and programs that make up a system, subsystem, or network.
<b>Content Panel</b>	One of the areas of the Web Administrator screen. The content panel displays settings, log information, and settings for the feature selected from the navigation panel.
<b>DACL</b>	Stands for discretionary access control list. It is used to control access by restricting a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.
<b>DHCP</b>	Stands for Dynamic Host Control Protocol. DHCP provides a mechanism by which a computer can acquire an IP address automatically when it connects to the network. DHCP allows more flexible and efficient use of network resources than static IP addresses.
<b>DN</b>	Stands for distinguished name. A distinguished name uniquely identifies an entry in the directory. A DN is made up of relative distinguished names (RDNs) of the entry and each of the entry's parent entries, up to the root of the directory tree. RDNs are usually separated by commas and optional spaces. For example: 'uid=JohnDoe, ou=People, dc=company, dc=com'.
<b>DNS</b>	Short for Domain Name Service. A network service that translates domain names into IP addresses. If you have multiple DNS servers on your network, and one DNS server can't translate a domain name, it asks another one, and so on, until the IP address is found. <i>See also</i> Domain Name System.
<b>Domain</b>	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
<b>Domain Name</b>	A name that identifies a domain. <i>See also</i> <i>Domain</i> . The domain name can be the company name, division name, facility name, department name, or other descriptive name.
<b>Domain Name System</b>	The network server that maintains the list of all host names in a domain. Sun StorEdge 5310 NAS Appliance uses the name server to translate domain names to the corresponding IP address. <i>See also</i> DNS.
<b>DTQ</b>	Stands for Directory Tree Quota. A directory tree quota is a quota, or limit, to the space or the number of files that a directory tree (a directory and its subdirectories) can occupy.
<b>Dual-head</b>	A reference to the Sun StorEdge 5310 Cluster system which consists of a pair of identical servers or "heads."
<b>Ethernet</b>	A network communication system developed and standardized by DEC, Intel, and Xerox using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for

integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber optics, broadband, and unshielded twisted pair.

**Failback** The recovery process from a failover state. If one head, controller, or network link fails, failover automatically transfers all functions of the failed unit to the working unit. Once the failed unit is repaired and is online, failback returns all RAID volume ownership and network interfacing functions to their pre-failover configuration. *See also* Failover.

**Failover** A feature that allows system-wide data redundancy in the event of a head, controller, or link failure. **Head failover** occurs when one head suffers a hardware failure that renders a data path unavailable. The working head automatically takes ownership of all operations of the failed head, including RAID volume ownership and network interface addressing. **Controller failover** allows a working RAID controller to take ownership of RAID volumes formerly managed by the failed controller. **Link failover** ensures that an alternate network link becomes active when a primary link fails. *See also* Failback.

**File Sharing** A feature that allows users of networked computers to make files available to other users.

**File Volume** File systems created from partitions that have available space. If the file volume does not use up all the available space in a partition, the remaining space is automatically allocated into the next partition. *See also* Partition.

**File Volume Extension** *See* Segment.

**Gateway** A combination of hardware and software that links two different types of networks. For example, the interconnection of an Ethernet network and a Token Ring network requires a gateway.

**Gateway Address** The gateway address is the IP address of one of the gateways or routers attached to the local network. Specifically, it is the IP address of a network server or host that functions as a gateway to other networks through communication lines or other network topologies.

**Gigabit Ethernet** An Ethernet standard that enables data transfer rates of up to 1 Gbps running over optical fiber cable.

**Group Membership** The list of groups to which a user belongs.

**GUI** Stands for Graphical User Interface. A GUI uses graphical elements to present information to a computer user rather than the traditional text-only command line interface still found in telnet and similar implementations.

- Head** In Sun StorEdge 5310 NAS Appliance a head is the server portion of the Sun StorEdge 5310 NAS Appliance system. A Sun StorEdge 5310 NAS Appliance consists of one or two heads and one or more RAID or drive units. The head controls the RAID or drive units and acts as a thin file server. See also *RAID* and *Thin File Server*.
- Hot Spare** A drive present in the system, but unused until another drive fails. At that time, the hot spare automatically takes over for the failed drive.
- HTTP** Stands for Hypertext Transmission Protocol. A protocol for exchanging HTML pages and forms.
- Hub** A physical layer device that restores the amplitude and timing of a signal. Also known as a concentrator.
- HTML** Stands for Hypertext Markup Language. HTML is a markup language used for creating Web pages. Markups, or commands, are embedded in a document and interpreted by a browser to format the document contents on the computer screen.
- Hyperlink** Also link. A reference from some point in one hypertext document to another document or another place in the same document. Links enable users to jump quickly to points of reference. Browsers display links in some distinguishable way—in different form, color, or style, for example. When a user activates a link, the browser displays the target on the link.
- Internet** The world's largest computer network.
- Intranet** A network internal to an organization, accessed through a browser but not necessarily connected to the Internet. The most common example is an information distribution network set up on Web servers within a company and providing only internal company access to the Web-based information.
- IP Address** A unique 32-bit value that identifies network hosts using TCP/IP. An IP address, or a block of addresses, is assigned upon application to organizations responsible for that function. No two network hosts can be assigned the same IP address. Each address consists of a network number, optional subnetwork number, and host number, written as four numbers separated by periods. Each number can be 0 to 255. See also *Address* and *URL*.
- Java programming language** Java is a programming language developed by Sun Microsystems to be portable to any type of computing device. In practice, java allows web browsers to do much more than display information. Java scripts allow much more flexibility and functionality in web access and they run on virtually any type of computer.
- Kerberos Realm** A kerberos realm is a secured network requiring access through a key. (See also *KDC*.) Each system or user with a key can access any services or systems that the key opens. The user does not have to enter a user name and password each time there is a controlled service request.

- KDC** Stands for Key Distribution Center. The KDC acts as the server and offers authentication to users, systems, and services (such as telnet, ftp, login, and e-mail) within its “realm”. See also *Kerberos Realm*.
- LAN** Stands for Local Area Network. A communications network that provides high-speed (over 1 Mbps) data transmission and is limited to a specific physical area (up to about six miles). The basic components of a LAN are: adapter boards installed in each computer to provide a cable connector, cabling, server hardware, and network management software.
- LCD** Stands for Liquid Crystal Display. An LCD is a display device used primarily for displaying small amounts of textual information. On the Sun StorEdge 5310 NAS Appliance, the LCD is a two line display that shows basic information about system functions and, in conjunction with the control panel, allows you to perform certain system functions, like setting the IP address, directly on the unit, without access through the internet or intranet.
- LDAP** Stands for Lightweight Directory Access Protocol and is a directory service protocol that runs over TCP/IP.
- Login** Logging in is a security process designed to prevent access to system settings or other resources by those who should not have access. A login process usually requires a user name and password to verify, or authenticate, a user.
- LUN** Refers to Logical Unit Number for SCSI interface components and peripherals. Used to identify the logical representation of a physical or virtual device, addressable through a target. A logical unit can have more than one physical device. *See also* SCSI.

#### **Master Domain**

**Model** One of several types of domain models. In the Master Domain Model, an account domain is trusted by a resource domain.

**NAS** Stands for Network Attached Storage.

#### **Name Service Lookup**

**Order** The sequence in which the available name services are searched to resolve a query. These name services can include NIS, NIS+, DNS, and Local.

#### **Navigation Panel**

The navigation panel is the region of the Web Administrator window that allows you to access the different functions of Web Administrator. The navigation panel is on the left side of the Web Administrator window. See also *Content Panel*.

**NDMP** Stands for Network Data Management Protocol.

**NetBIOS** NetBIOS is a BIOS used for networking. NetBIOS was designed to support communications between symbolically named stations and the transfer of arbitrary data. NetBIOS manages the use of node names and transport layer connections for higher layer protocols such as SMB.

<b>Netmask</b>	Used to indicate which portion of an IP address identifies the network address and which portion identifies the host address.
<b>Network</b>	A series of nodes such as terminals, computer systems, or other peripheral devices connected by a communications channel. <i>See also</i> LAN.
<b>Network Address</b>	An IP address assigned to a network that permits access by other networks. Refers to a logical, rather than a physical, network device.
<b>Network Class</b>	There are three network classes, identified as Type A, Type B, or Type C. The class type is determined by the number of network hosts in the network. Small networks are Type C and the largest networks are Type A. Type A networks can contain thousands of network hosts.
<b>Network Host</b>	A network server or workstation.
<b>NIC</b>	Stands for Network Interface Card. A NIC is an expansion card that provides access to a network.
<b>NIS</b>	Short for Network Information Service. Along with NFS, NIS provides a distributed database system to centralize (i.e, store one copy, on a single computer) common configuration files, such as the password file (/etc/passwd) and the hosts file (/etc/hosts).
<b>NIS+</b>	Short for Network Information Service Plus (NIS+). NIS+ was designed to replace NIS, and is the new default naming service for the Solaris OS. NIS+ can provide limited support to NIS clients, but was mainly designed to address problems that NIS cannot address.
<b>Node</b>	A device connected to the network and capable of communicating with other network devices.
<b>NTP</b>	Stands for Network Time Protocol. NTP provides a mechanism for synchronizing the time among a number of computers connected to a network.
<b>Option Button</b>	An option button is a screen control that allows you to select one option out of a predefined group of mutually exclusive options. Option buttons are also called <i>Radio Buttons</i> .
<b>Packet</b>	A piece of a message transmitted over a network. Contains the destination address in addition to the data. Once all packets arrive at the destination, they are recompiled into the original message.
<b>Partition</b>	Sections on a LUN. Each partition can either have some space allocated to it, or can be empty. When a LUN is first created, all of the available space is located in the first partition, while the other partitions are empty. Each partition can have only one volume.
<b>Port Bonding</b>	Otherwise known as “channel bonding.” Port bonding allows you to scale network I/O by joining ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth.

- Protocol** A set of standards or rules that enable computers to connect to one another and exchange data. Using a protocol helps reduce the possibility of errors during data transmission.
- Quota** A restriction on disk space or the number of files written to file volumes in the Sun StorEdge 5310 NAS Appliance. This limit can be determined for a user or group (user or group quota) or for a directory (directory tree quota).
- Radio Button** A radio button is a type of screen control that allows you to select one choice from a predefined group of mutually exclusive choices. See also *Option Button*.
- RAID** Stands for Redundant Array of Independent Disks.
- RDATE** RDATE is a time synchronization method that simply asks another computer on the network what the correct time is and resets itself accordingly. RDATE is not particularly accurate, but is adequate for most networks.
- Realm** See also *Kerberos Realm*. A realm is a secured portion of a network that uses the kerberos method for verifying users and access rights.
- RPC** Stands for remote procedure call. An easy and popular paradigm for implementing the client-server model of distributed computing. A request is sent to a remote system to execute a designated procedure, using arguments supplied, and the result is returned to the caller.
- Scope** Scope is a method used in Windows NT environments for subdividing workgroups into more manageable sections, without breaking up the ability of the workgroup to exchange information readily.
- SCSI** SCSI stands for Small Computer System Interface. SCSI is a standard interface for computers that allows connection of up to 15 peripheral devices (such as disk drives or a tape backup device) to be interconnected in a daisy-chain configuration. The basic SCSI standard is twenty-five years old. However, it has been updated and expanded many times. The original 5 Mbps data transfer rate has been expanded to 320 Mbps and many features have been added. See also LUN.
- SCSI ID** Priority number (address) of a SCSI device in a SCSI device chain. Only one device at a time can transmit through a SCSI channel and priority is given to the device with the highest address. SCSI IDs range from 0 to 15 and each SCSI device must be given a unique and unused SCSI ID.
- Segment** Segments are available space that can be “attached” to a volume when the volume reaches its assigned capacity. This increases the volume’s total capacity. The segment, after being attached, becomes part of the volume and cannot be removed. Otherwise known as volume extensions.
- Server** A network host that makes network resources, such as software applications and databases on hard disk or CD-ROM, available to network users. The server provides the centralized, multi-user functionality of the network application, such as data management, information sharing, network administration, or security.

<b>Server Name</b>	Identifies a network server. Server names are used in addition to IP addresses. This allows a server to be advertised on a network with a recognizable name. For example, the first Sun StorEdge 5310 NAS Appliance server on a network could be identified as <i>cdts0</i> , the second as <i>cdts1</i> , and the third as <i>cdts2</i> or they could be identified as Fred, Barney, and Wilma.
<b>SFS</b>	Stands for Server File System. The name of the file system used by the Sun StorEdge NAS Appliance products.
<b>Shutdown</b>	The multi-user operating system resident on the Sun StorEdge 5310 NAS Appliance server must be shut down in an orderly sequence prior to turning the power off. The shutdown sequence closes files and terminates running programs to prevent loss or corruption of data.
<b>Single Domain Model</b>	Refers to a domain model in which the resource and account domains are on the same network with no trust relationship.
<b>Single-head</b>	A reference to the Sun StorEdge 5310 NAS Appliance which consists of a single server or "head."
<b>SMB</b>	Stands for Server Message Block. A Microsoft-compatible network protocol for exchanging files. SMB is typically used by Windows for Workgroups, OS/2 Warp Connect, and DEC Pathworks. <i>See also</i> CIFS.
<b>SNMP</b>	Stands for Simple Network Management Protocol. SNMP is primarily used for network monitoring and notification of network errors and other events. In the Sun StorEdge 5310 NAS Appliance, SNMP also provides notification services through email messages.
<b>Subnet</b>	A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons.
<b>System Events Panel</b>	The system events panel is the bottom portion of the Web Administrator window. This panel displays information about system events at all times.
<b>TCP/IP</b>	A commonly used networking protocol that allows interconnection of different network operating systems. Stands for Transmission Control Protocol/Internet Protocol.
<b>Telnet</b>	A terminal emulation program for TCP/IP networks. The Telnet program runs on your computer and connects your PC to the Sun StorEdge 5310 NAS Appliance server on the network. You can then enter commands through the Telnet program and they run as if you were entering them directly on the server console.
<b>Thin File Server</b>	A server designed for the specific function of serving files but not applications.

- Toolbar** The toolbar is the portion of the Web Administrator window directly beneath the title bar. It contains icons that access several common tools. For more information, see "The Toolbar" on page 10.
- UNC** Stands for Universal Naming Convention. The UNC refers to the standard method of defining the location of shares on a computer and consists of a computer name and share name. For example, \\acctng1\jeremy.
- Unicode** Unicode is a standard for representing letters that allows the language of computer messages and commands to be displayed in a variety of languages without rewriting the underlying programs.
- URL** Stands for Uniform Resource Locator. An address system used by servers and clients to request documents. See also *IP Address*.
- User Credentials** The information containing the user, account data, and the user's group membership.
- VLAN** Stands for Virtual Local Area Network. A VLAN acts like an ordinary LAN, but connected devices don't have to be physically connected to the same segment.
- WAN** Stands for Wide Area Network. A large (geographically disperse) network.
- Web Browser** A web browser is a software application designed to search for and retrieve information from the Internet and the world-wide web. See also *Internet*, *Intranet*, and *WWW*.
- WINS** Stands for Windows Internet Naming Service. A WINS server resolves NetBIOS names to IP addresses, allowing computers on a network to locate other NetBIOS devices more quickly and efficiently. WINS performs a similar function for Windows environments as DNS does for UNIX environments.
- Workgroup** A portion of a network identified by a workgroup name that is used to organize network hosts by function, department, or other designation. For example, workgroups can be created for departments such as accounting, shipping, and marketing.
- Workstation** A computer on a network intended for user access to network resources.
- WWW** Stands for World Wide Web. An Internet, client-server, hypertext-distributed information retrieval system.



# Index

---

## NUMERICS

100Base-TX, defined 285

10Base-T, defined 285

## A

### About

ADS 79, 80

autohome shares 117

checkpoints 188

consistency spots 188

controller failover 184

c-spots 188

DNS 79

file volume 49

group privileges 94

head failover 24, 184

IP aliasing 64

LDAP 79

LUN 48

mirroring 136

NIS 79

NIS+ 79

partition 49

RAID 47

routes 169

segment 50

shares 109

static shares 109

Sun StorEdge 5310 NAS Appliance 1

SysMon 263

time synchronization 58

user groups 93

User's Guide 3

warning thresholds 142

WINS 79

Access control, defined 285

Access rights, defined 94, 285

Accessing

checkpoints 198

Acquiring IP address

dynamically 5

manually 5

Action button, defined 285

Activating, options 133

Active Directory Service

see ADS

Active server

configuring

GUI 137

mirroring

defined 136

Active/Active cluster, defined 285

Activity monitor, viewing, telnet 250

Adapters, network, configuring

GUI 27

telnet 209

Adding

checkpoints

GUI 188

telnet 260

directory tree quotas 125

file volume

telnet 224

- group members
  - GUI 96
  - telnet 236
- group quotas 120
- hosts
  - GUI 99
  - telnet 242
- NFS exports 129
- scheduled checkpoint 191
- segment
  - telnet 227
- static shares
  - GUI 111
  - telnet 232
- trusted hosts
  - GUI 99
  - telnet 244
- user quotas 120

Address, defined 285

Administrator
 

- group 94

ADS
 

- about 79, 80
- configuring
  - GUI 81
  - telnet 234
- Windows 2000 clients 117
- container names 83
- defined 14, 285
- enabling 81
- publishing shares 86
- removing shares 87
- setting up
  - GUI 32, 81
  - telnet 234
- updating share containers 87

Aggregating
 

- see Bonding ports

Alert
 

- events, system log 160
- mirror buffer thresholds 143

Alias IP address
 

- about 64
- defined 285

Alternate gateway, defined 286

Assigning
 

- language 44
- port roles 29
- server name 18

Attaching segments
 

- telnet 227

Auth, log facility 44

Authentication, defined 286

Autohome shares
 

- about 117
- configuring 118
- defined 286
- setting up, telnet 231

## B

Backup
 

- cleaning the heads 200
- NDMP
  - GUI 199
- operators group 94
- viewing
  - job status 176
  - log 175
  - tape status 176

BIOS, defined 286

Bonding ports 65
 

- dual-head systems 68
- dual-head, example 70
- viewing, telnet 252

Boot up, defined 286

Breaking mirrors
 

- GUI 144
- server 1
  - GUI 147

Broadcast address, defined 286

Browser
 

- defined 286

## C

### Changing

- directory tree quotas 127
- group quotas 122
- hosts
  - GUI 100
  - telnet 243
- language
  - telnet 215
- mirrors 141
- name services lookup order
  - GUI 89
  - telnet 222
- NFS exports 131
- partition names, telnet 227
- scheduled checkpoint 193
- static shares
  - GUI 115
  - telnet 233
- trusted hosts 100
- user quotas 122

### Channel bonding

- see bonding ports

### Checkpoints

- about 188
- accessing 198
- adding to schedule
  - GUI 191
  - telnet 260
- analysis, viewing from telnet 253
- creating 188
- editing the schedule 193
- removing 195
- removing scheduled 194
- renaming 194
- scheduling
  - GUI 190
  - telnet 260
- sharing 195

### CIFS

- autohome shares
  - configuring 118
  - setting up, telnet 231
- Compliance Archiving Software 261
- configuring clients
  - DOS 117
  - Windows 116
- defined 109, 286

- drive letter mapping 223
- share name limits 112, 115
- static shares
  - about 109
  - adding 111
  - configuring 110
  - creating 111
  - editing 115
  - removing 116
  - security 113
  - setting up, telnet 230

### Clients

- configuring 116
- DOS 117
- Windows 116

### Cluster, defined 286

### Common Internet File System

- see CIFS

### Compliance Archiving Software 152

- API 269
- configuring 261

### Compliance, defined 286

### Configuration, defined 287

### Configuring

- active server
  - GUI 137

### ADS

- GUI 32, 81
- telnet 234

### autohome shares

- GUI 118
- telnet 231

### Compliance Archiving Software 261

### date

- GUI 61
- telnet 211

### directory tree quotas 124

### DNS

- GUI 34
- telnet 218

### drive letters in telnet 223

### dynamic DNS

- telnet 218

### email notification

- GUI 41
- telnet 248

### failback

- telnet 258

- failover
  - GUI 185
  - telnet 257
- FTP
- gateway address 30
- group
  - privileges 94
  - privileges, telnet 237
  - quotas 119
- hosts
  - GUI 99
- initial Sun StorEdge 5310 NAS Appliance
  - configuration 4
- language
  - GUI 44
  - telnet 215
- LDAP
  - GUI 88
- local logging
  - GUI 43
  - telnet 218
- mirror server
  - GUI 137
- mirroring file volumes
  - GUI 139
- name services
  - GUI 40
  - telnet 218
- NDMP
  - GUI 199
- network adapters 27
- NFS exports 128
- NICs 27
- NIS
  - GUI 36
  - telnet 221
- NIS+
  - GUI 38
  - telnet 221
- NTP
  - GUI 59
  - telnet 212
- ports
  - GUI 27
  - mirroring 138
  - telnet 209
- privileges
  - GUI 98
  - telnet 237
- RDATE
  - GUI 60
  - telnet 214
- remote logging
  - GUI 43
  - telnet 218
- running the wizard 13
- server name 18
- SMB/CIFS clients 116
- SMTP
  - telnet 249
- SNMP
  - GUI 155
  - telnet 247
- source server
  - GUI 137
- starting the wizard 14
- static shares
  - GUI 110
  - telnet 230
- target server
  - GUI 137
- TCP/IP
  - telnet 208
  - with DHCP 5
  - without DHCP 5
- time
  - GUI 61
  - telnet 211
- time synchronization
  - GUI 59
  - telnet 212
- time zone
  - GUI 61
  - telnet 211
- user groups, telnet 235
- user quotas 119
- variations of the wizard 13
- verifying DNS for ADS 85
- warning thresholds 142
- Windows security 31
- WINS 33
- Connecting to Web Administrator 7
- Consistency spots, about 188
- Contacting Technical Support 282
- Containers, updating ADS shares 87

- Content panel
  - defined 287
  - using 12
- Controller
  - failover, about 184
  - failover, enabling 185
  - information, viewing 172
- Conventions
  - server names 18
  - used in this guide 3
- Creating
  - checkpoints
    - GUI 188
    - telnet 260
  - directory tree quotas 125
  - file volume
    - GUI 50
    - telnet 224
  - group quotas 120
  - hosts
    - GUI 99
    - telnet 242
  - NFS exports 129
  - scheduled checkpoint
    - GUI 191
    - telnet 260
  - segment
    - GUI 50
    - telnet 227
  - static shares
    - GUI 111
    - telnet 232
  - trusted hosts
    - GUI 99
    - telnet 244
  - user quotas 120
- Credentials, mapping 101
- Critical events, system log 160
- C-spots, about 188

## D

- Daemon, log facility 44
- Date, setting
  - GUI 61
  - telnet 211
- Debug events, system log 160
- Dedicated port
  - mirroring 138
  - setting port role 138
- Default quotas
  - group 119
  - user 119
- Defining
  - file volume 50
  - segment 50
- Deleting
  - checkpoint 195
  - directory tree quotas 128
  - file volume
    - telnet 229
  - group members
    - GUI 96
    - telnet 237
  - hosts
    - GUI 101
    - telnet 244
  - NFS exports 132
  - out-of-date file volume
    - GUI 148
  - scheduled checkpoint 194
  - static shares
    - GUI 116
    - telnet 233
  - trusted hosts
    - GUI 101
    - telnet 245
  - user quotas 124
- DHCP
  - configuring TCP/IP 5
  - defined 5, 287
  - disabling with head failover 24
- Diagnostic email, sending 281
- Directory tree quotas
  - adding 125
  - configuring 124
  - deleting 128
  - editing 127
- Displaying
  - routes 170
  - system events 160
  - system log 158
- DN, defined 32

- DNS
    - about 79
    - defined 5, 287
    - setting up
      - GUI 34
      - telnet 218
    - verifying configuration 85
  - Documentation
    - conventions 3
    - set 2
  - Domain
    - defined 287
    - security 31
  - Domain Name Server
    - defined 287
    - see DNS
  - Domain name, defined 287
  - DOS, configuring for SMB/CIFS 117
  - Down timeout, defined 25, 186
  - Drive letters, configuring, telnet 223
  - DTQ
    - defined 124, 287
    - see Directory tree quota
  - Dual-head systems
    - bonding ports 68
    - enabling head failover 24
      - telnet 257
    - IP aliases 64
    - port bond example 70
    - port roles 29
  - Dual-head, defined 287
  - Dynamic DNS
    - enabling 35
    - setting up, telnet 218
  - Dynamic Host Configuration Protocol
    - see DHCP
  - Dynamic IP address acquisition 5
- E**
- Editing
    - directory tree quotas 127
    - group quotas 122
    - hosts
      - GUI 100
      - telnet 243
    - keys used in telnet 206
    - mirrors 141
    - NFS exports 131
    - scheduled checkpoint 193
    - static shares
      - GUI 115
      - telnet 233
    - trusted hosts 100
    - user quotas 122, 124
  - Email notification
    - configuring, telnet 248
    - diagnostic, sending 281
    - notification levels 42
    - setting up 41
  - Emergency events, system log 160
  - Enabling
    - ADS
      - GUI 81
      - telnet 234
    - autohome shares
      - GUI 118
      - telnet 231
    - checkpoints
      - telnet 260
    - controller failover
      - GUI 185
      - telnet 257
    - DNS
      - GUI 34
      - telnet 218
    - domain security 31
    - dynamic DNS
      - GUI 35
      - telnet 218
    - email notification
      - GUI 41
      - telnet 248
    - failover
      - GUI 24
      - telnet 257
    - foreign languages
      - GUI 44
      - telnet 215
    - group quotas
      - GUI 120
      - telnet 235

- head failover
  - GUI 185
  - telnet 257
- LDAP
  - GUI 88
- link failover
  - GUI 25
  - telnet 257
- local logging
  - GUI 43
  - telnet 218
- name services
  - GUI 40
  - telnet 218
- NIS
  - GUI 36
  - telnet 221
- NIS+
  - GUI 38
  - telnet 221
- quotas
  - telnet 235
- remote logging
  - GUI 43
  - telnet 218
- SNMP
  - GUI 156
  - telnet 247
- static shares
  - GUI 111
  - telnet 230
- UPS monitoring 172
- user quotas
  - GUI 120
  - telnet 235
- WINS 33
- workgroup security 32

Environmental status

- system fans 161
- system power supplies 163
- temperature 162
- viewing 161
- voltage 164

Error events, system log 160

Error messages 263

- file system errors 266
- IPMI events 267
- RAID subsystem errors 266

- SysMon 263
- UPS subsystem errors 264

Establishing a file system 50

Ethernet, defined 287

Events

- IPMI 267
- logging in telnet 219
- system log 160

Example dual-head port bond 70

Exports

- creating 129
- editing 131
- removing 132
- setting up 128

## **F**

Facility

- remote logging 44
- telnet 219

Failback

- configuring
  - telnet 258
- defined 288
- initiating
  - GUI 26, 186

Failover

- configuring, telnet 257
- controller
  - about 184
  - enabling 185
- defined 288
- enabling 24
- head
  - about 24, 184
  - enabling 185
- link, enabling 25
- managing, telnet 256

Fan

- status 161

Fault tolerance, failover

- head, about 24
- link, enabling 25

File directory security 104

File Replicator 136

File sharing, defined 288

- File system
  - error messages 266
  - establishing 50
  - managing in telnet 223
- file system errors 266
- File Transfer Protocol
  - see FTP
- File volume
  - about 49
  - autohome shares
    - about 117
    - telnet 231
  - creating
    - GUI 50
    - telnet 224
  - defined 288
  - deleting
    - telnet 229
  - deleting out-of-date volume
    - GUI 148
  - expanding
    - telnet 227
  - managing access, telnet 246
  - mirroring
    - GUI 139
  - mirroring up-to-date volume
    - GUI 149
  - name limits 52
  - promoting
    - GUI 145
  - re-establishing mirror
    - GUI 146
  - static shares
    - about 109
    - telnet 230
  - usage statistics 165
- File volume extension
  - see Segment
- FTP
  - access 182, 254
- FTP, configuring

## G

- Gateway address
  - defined 288
  - setting 30

- Gateway, defined 30, 288
- GID, defined 113
- Gigabit ethernet, defined 288
- Graphical user interface
  - see GUI
- Group
  - adding members
    - GUI 96
    - telnet 236
  - administrators 94
  - backup operators 94
  - credentials, mapping 101
  - membership, defined 288
  - power users 94
  - privileges
    - GUI 94
    - telnet 237
  - quotas
    - adding 120
    - configuring 119
    - default 119
    - deleting 124
    - editing 122
  - removing members
    - GUI 96
    - telnet 237
  - root
    - hard limits 119
    - quotas 119
    - soft limits 119
  - user, about 93
- GUI
  - content panel 12
  - defined 1, 288
  - navigation panel 11
  - online help 13
  - system events panel 13
  - toolbar 10
  - using 9

## H

- Halt the server 183
- Hard limits 119
- Head
  - cleaning 200
  - defined 24, 289



- failover
  - about 184
  - described 24
  - enabling 185
- Help, using 13
- Hosts
  - adding
    - GUI 99
    - telnet 242
  - configuring 99
  - deleting, telnet 244
  - editing
    - GUI 100
    - telnet 243
  - naming 100, 101
  - removing 101
  - routes 169
  - trusted
    - adding, telnet 244
    - configuring 99
    - deleting, telnet 245
    - editing 100
    - GUI 99
    - removing 101
    - telnet 244
- Hot spare
  - defined 289
- HTML, defined 289
- HTTP, defined 289
- Hub, defined 289
- Hyperlink, defined 289

**I**

- Icons, toolbar 10
- Identifying port locations 27, 63
- Immediate
  - checkpoints, creating 188
- Independent, port role 63
- Information events, system log 160
- Initial configuration, Sun StorEdge 5310 NAS Appliance 4

- Initiating
  - controller recovery 26, 186
  - failback
    - GUI 26, 186
  - head recovery 26, 186
- Internet, defined 289
- Intranet, defined 289
- IP address
  - aliasing 64
  - defined 289
  - entering through LCD panel 5
  - options for providing 4
- IP aliases
  - about 64
  - dual-head systems 64
- IPMI
  - event messages 267
- IPMI events 267

## **J**

- Java
  - defined 289

## **K**

- KDC, defined 33, 290
- Kerberos realm, defined 289
- Kern, log facility 44
- Key distribution center
  - see KDC

## **L**

- LAN, defined 290
- Language
  - assigning 44
  - selecting, telnet 215
- LCD
  - defined 5, 290
  - entering IP address 5

- LDAP
    - about 79
    - configuring
      - GUI 88
    - enabling 88
    - setting up
      - GUI 88
  - Lightweight Directory Access Protocol
    - see LDAP
  - Limits
    - hard 119
    - names
      - ADS container 83
      - container 83
      - domain 31
      - file volume 52
      - host 100, 101
      - NetBIOS 31
      - scope 34
      - segment 52
      - server 18
      - share 112, 115
    - soft 119
  - Link failover, enabling 25
  - Liquid Crystal Display
    - see LCD
  - Local
    - log facility 44
    - logging
      - setting up 43
      - telnet 218
  - Locking the console 247
  - Logging
    - alert events 160
    - backup log
      - GUI 175
    - configuring 43
    - critical events 160
    - debug events 160
    - displaying the log 158
    - emergency events 160
    - enabling 43
    - error events 160
    - event types 219
    - facilities
      - GUI 44
      - telnet 219
    - information events 160
    - local, setting up
      - telnet 218
    - notice events 160
    - remote, setting up
      - telnet 218
    - setting up 43
    - system events 160
    - viewing system log
      - GUI 158
      - telnet 251
    - warning events 160
  - Logical unit number
    - see LUN
  - Login
    - defined 290
    - procedure 8
    - Web Administrator 8
  - Lookup order
    - changing 89
    - name services, verifying 84
    - setting in telnet 222
  - LUN
    - about 48
    - defined 48, 290
    - rebuilding 73
  - LUN path 20
    - about 19
    - dual-head system 21
    - setting 22
- ## M
- MacIntosh
    - desktop DB calls 112, 115
    - support 112, 115
  - Mail, log facility 44
  - Main menu, telnet 206
  - Managing
    - failover, telnet 256
    - file volume access, telnet 246
    - quotas 119
    - routes, telnet 215
    - trusted hosts, telnet 244
  - Manual IP address acquisition 5

- Mapping
  - credentials 101
  - drive letters, telnet 223
- Master domain model, defined 290
- Messages
  - display language 44
- Mirror
  - buffer
    - defined 136
    - threshold alerts 143
  - port role 64
  - server
    - configuring 137
    - defined 136
    - setting up 137
- Mirroring
  - about 136
  - active server, defined 136
  - before you begin 136
  - breaking
    - mirror 144
  - changing 141
  - configuring
    - dedicated port 138
  - defined 48
  - editing 141
  - mirror buffer, defined 136
  - mirror server, defined 136
  - promoting file volume
    - GUI 145
  - re-establishing a mirror
    - GUI 146
  - requirements 136
  - setting up
    - dedicated port 138
    - file volumes 139
  - source server, defined 136
  - status states 174
  - target server, defined 136
  - usage statistics 172
- Modifying, telnet
  - group privileges 237
- Monitoring
  - configuring SNMP 155
  - UPS 170
    - enabling 172

## N

- Name
  - container, limits 83
  - domain 31
  - file volume 52
  - hosts 100, 101
  - NetBIOS limitation 31
  - scope 34
  - segment 52
  - server
    - conventions 18
    - setting 18
  - share name limits 112, 115
- Name services
  - changing lookup order 89
  - configuring 40
  - DNS 40
  - enabling 40
  - Local 40
  - lookup order, defined 290
  - NIS 40
  - NIS+ 40
  - setting lookup order, telnet 222
  - setting up 40
  - verifying lookup order 84
- Navigating
  - telnet 206
  - Web Administrator 8
- Navigation panel
  - defined 290
  - using 11
- NDMP
  - defined 199
  - setting up 199
- NetBIOS, defined 290
- Netmask, defined 291
- Network
  - activity, usage statistics 166
  - address, defined 291
  - class, defined 291
  - Data Management Protocol
    - see NDMP
  - defined 291
  - File System
    - see NFS
  - host, defined 291
  - Information Service
    - see NIS

- Information Service Plus
  - see NIS+
- interface card
  - see NIC
- routes 169
  - displaying 170
  - statistics 169
- Time Protocol
  - see NTP

- NFS
  - defined 128
  - exports
    - creating 129
    - editing 131
    - removing 132
    - setting up 128

- NIC
  - configuring 27
  - defined 27, 291

- NIS
  - about 79
  - defined 15, 291
  - setting up
    - GUI 36
    - telnet 221

- NIS+
  - about 79
  - defined 15, 291
  - setting up
    - GUI 38
    - telnet 221

- Node, defined 291

- Normal login 8

- Notice events, system log 160

- Notification levels, email notification 42

- NSSLDAP, see LDAP

- NTP
  - defined 58, 291
  - setting up
    - GUI 59
    - telnet 212
  - time synchronization
    - GUI 58
    - telnet 212

## O

- Online help, using 13

- Option button, defined 291

- Options

- activating 133
- Compliance Archiving Software 152, 261
- Compliance Archiving Software, API 269
- mirroring 136

- Ownership assignment, group privilege 95

## P

- Packet, defined 291

- Parity, defined 48

- Partition

- about 49
- defined 291
- renaming, telnet 227

- Password

- administrator, setting 57

- Path names, ADS 83

- Ports

- activity, usage statistics 168
- bonding 65
  - defined 291
  - dual-head systems 68
  - dual-head, example 70
- configuring
  - telnet 209
- location
  - identifying 27, 63
- mirroring
  - configuring 138
  - setting up 138
- roles 64
  - assigning 29
  - independent 63
  - mirror 64
  - primary 63
  - private 64
  - setting dedicated port 138
  - viewing port bonds, telnet 252

- Power supply
  - status 163

- Power users group 94

- Primary, port role 63

- Private, port role 64
- Privileges
  - configuring 98
  - defined 94
  - ownership assignment 95
  - root user 99
  - user groups 94
- Promoting
  - file volume
    - GUI 145
- Protocol, defined 292
- Providing, IP address 4
- Publishing shares in ADS 86

## Q

- Quotas
  - default group 119
  - default user 119
  - defined 292
  - directory tree
    - adding 125
    - configuring 124
    - deleting 128
    - editing 127
  - enabling
    - telnet 235
  - group
    - adding 120
    - configuring 119
    - deleting 124
    - editing 122
  - hard limits 119
  - managing 119
  - root group 119
  - root user 119
  - soft limits 119
  - user
    - adding 120
    - configuring 119
    - deleting 124
    - editing 122, 124

## R

- Radio button, defined 292
- RAID
  - about 47
  - defined 47
  - error messages 266
  - levels supported 47
  - sets 47
- RAID subsystem errors 266
- RDATE
  - defined 292
  - setting up
    - GUI 60
    - telnet 214
  - time synchronization
    - GUI 58
    - telnet 214
- Realm, defined 292
- Rebooting
  - server 183
  - telnet 256
- Rebuilding, LUN 73
- Recovery
  - initiating 26, 186
- Redundant Array of Independent Disks
  - see RAID
- Re-establishing a mirror
  - breaking the mirror
    - GUI 147
  - deleting out-of-date file volume
    - GUI 148
  - GUI 146
  - mirroring up-to-date file volume
    - GUI 149
- Remote logging
  - facilities 44
  - setting up
    - GUI 43
    - telnet 218
- Removing
  - checkpoint 195
  - directory tree quotas 128
  - file volume
    - telnet 229
  - group members
    - GUI 96
    - telnet 237

- group quotas 124
- hosts
  - GUI 101
  - telnet 244
- NFS exports 132
- scheduled checkpoint 194
- shares from ADS 87
- static shares
  - GUI 116
  - telnet 233
- trusted hosts
  - GUI 101
  - telnet 245
- Renaming
  - checkpoint 194
  - partitions, telnet 227
- Requirements
  - mirroring 136
  - server name 18
  - software 4
- Restore
  - cleaning the heads 200
  - timeout, defined 25, 186
- Retention period, Compliance Archiving Software 261
- Root group
  - hard limits 119
  - quotas 119
  - soft limits 119
- Root user
  - hard limits 119
  - privileges defined by host status 99
  - quotas 119
  - soft limits 119
- Routes
  - about 169
  - displaying 170
  - flags 169
  - host 169
  - managing in telnet 215
- Running
  - configuration wizard 13
  - head cleaning 200

## S

- Scheduling
  - checkpoints 190
    - adding 191
    - editing 193
    - removing 194
    - telnet 260
- Scope, defined 292
- SCSI ID, defined 292
- SCSI, defined 292
- Security
  - administrator password 57
  - file volume access, telnet 246
  - locking the console 247
  - setting 105
  - static shares 113
  - unlocking the console 247
  - Windows 31
- Segment
  - about 50
  - adding, telnet 227
  - attaching
    - telnet 227
  - creating 50
  - defined 292
  - name limits 52
- Selecting language, telnet 215
- Sending a diagnostic email 281
- Server
  - defined 292
  - head, defined 24
  - Message Block
    - see SMB
  - name
    - conventions 18
    - defined 293
    - setting 18
  - reboot 183
- Setting
  - administrator password 57
  - date
    - GUI 61
    - telnet 211
  - gateway address 30
  - group quotas 119
  - language
    - telnet 215

- name services lookup order
  - GUI 40
  - telnet 222
- security 105
- server name 18
- time
  - GUI 61
  - telnet 211
- time zone
  - GUI 61
  - telnet 211
- user quotas 119
- warning thresholds
  - GUI 142
- Setting up
  - active server
    - GUI 137
  - ADS
    - GUI 32, 81
    - telnet 234
  - autohome shares
    - GUI 118
    - telnet 231
  - Compliance Archiving Software 261
  - controller recovery 26, 186
  - directory tree quotas 124
  - DNS
    - GUI 34
    - telnet 218
  - drive letters, telnet 223
  - dynamic DNS
    - telnet 218
  - email notification
    - GUI 41
    - telnet 248
  - failback 26, 186
  - failover, telnet 257
  - FTP
  - group privileges 94
  - head recovery 26, 186
  - hosts 99
  - language 44
  - LDAP
    - GUI 88
  - local logging
    - GUI 43
    - telnet 218
  - mirror server
    - GUI 137
  - mirroring file volumes 139
  - name services 40
  - NDMP
    - GUI 199
  - network adapters 27
  - NFS exports 128
  - NICs 27
  - NIS
    - GUI 36
    - telnet 221
  - NIS+
    - GUI 38
    - telnet 221
  - NTP
    - GUI 59
    - telnet 212
  - ports
    - GUI 27
    - mirroring 138
    - telnet 209
  - privileges 98
  - RDATE
    - GUI 60
    - telnet 214
  - remote logging
    - GUI 43
    - telnet 218
  - SMB/CIFS clients 116
  - SNMP
    - GUI 155
    - telnet 247
  - source server
    - GUI 137
  - static shares
    - GUI 110
    - telnet 230
  - target server
    - GUI 137
  - TCP/IP, telnet 208
  - time synchronization
    - GUI 59
    - telnet 212
  - Windows security 31
  - WINS 33

- Shares
  - about 109
  - autohome
    - about 117
    - configuring 118
    - setting up, telnet 231
  - checkpoints 195
  - mapping drive letters 223
  - naming limits 112, 115
  - publishing in ADS 86
  - removing from ADS 87
  - static
    - about 109
    - adding, telnet 232
    - configuring 110
    - creating 111
    - deleting, telnet 233
    - editing 115
    - editing, telnet 233
    - removing 116
    - security 113
    - setting up, telnet 230
  - updating ADS containers 87
- Shut down
  - defined 293
  - telnet 256
- Shutting down 183
- Simple Mail Transfer Protocol
  - see SMTP
- Simple Network Management Protocol
  - see SNMP
- Single domain model, defined 293
- Single-head, defined 293
- SMB
  - autohome shares
    - configuring 118
    - enabling 118
  - configuring
    - clients 116
    - DOS clients 117
    - Windows clients 116
  - defined 109, 293
  - drive letter mapping 223
  - security, static shares 113
  - setting up
    - autohome shares, telnet 231
    - static shares, telnet 230
  - share name limits 112, 115
  - static shares
    - about 109
    - adding 111
    - changing 115
    - configuring 110
    - creating 111
    - deleting 116
    - editing 115
    - enabling 111
    - removing 116
- SMTP
  - defined 41
- SNMP
  - configuring
    - GUI 155
    - telnet 247
  - defined 155, 293
- Soft limits 119
- Software
  - File Replicator 136
  - mirroring 136
  - requirements 4
  - supported 4
  - updating 201
- Source server
  - configuring
    - GUI 137
  - mirroring
    - defined 136
- Static shares
  - about 109
  - configuring 110
  - creating 111
  - editing 115
  - name limits 112, 115
  - removing 116
  - security 113
- Status 157
  - backup jobs 176
  - backup tapes 176
  - controller information 172
  - environmental, viewing 161
  - fans 161
  - file volume usage 165
  - mirror states 174
  - mirroring
    - GUI 172
  - network activity 166



- network routes 169
- port activity 168
- power supplies 163
- system activity 166
- temperature 162
- UPS 170
- voltage 164
- Striping, defined 48
- Subnet, defined 293
- Sun StorEdge 5310 NAS Appliance
  - initial configuration 4
  - introduction 1
  - software requirements 4
- Sun StorEdge File Checkpoints, see Checkpoints
- Supported RAID levels 47
- Synchronizing time
  - about 58
  - setting up 59
  - telnet 212
- Syslog, log facility 44
- SYSLOGD, defined 43
- SysMon, about 263
- System
  - activity usage statistics 166
  - events
    - displaying 160
    - panel, defined 293
    - panel, using 13
  - log
    - displaying 158
    - viewing, telnet 251
  - shutting down
    - GUI 183
    - telnet 256

## T

- Target server
  - configuring
    - GUI 137
  - defined 136
- TCP/IP
  - configuring
    - telnet 208
    - with DHCP 5
    - without DHCP 5

- defined 293
- Technical Support, contacting 282
- Telnet
  - adding
    - checkpoints 260
    - group members 236
    - hosts 242
    - segments 227
    - shares 232
    - trusted hosts 244
  - configuring
    - drive letters 223
    - email notification 248
    - failback 258
    - failover 257
    - SNMP 247
    - TCP/IP 208
    - user groups 235
  - creating file volumes 224
  - defined 293
  - deleting
    - file volume 229
    - hosts 244
    - shares 233
    - trusted hosts 245
  - edit keys 206
  - editing
    - hosts 243
    - shares 233
  - enabling quotas 235
  - locking console 247
  - logging
    - events 219
    - facilities 219
  - main menu 206
  - managing
    - failover 256
    - file system 223
    - file volume access 246
    - routes 215
    - trusted hosts 244
  - menus 206
  - modifying
    - group privileges 237
  - navigating 206
  - rebooting 256
  - removing group members 237
  - renaming partitions 227

- scheduling
  - checkpoints 260
- selecting, language 215
- setting
  - date 211
  - name services lookup order 222
  - time 211
  - time synchronization 212
  - time zone 211
- setting up
  - ADS 234
  - autohome shares 231
  - DNS 218
  - dynamic DNS 218
  - local logging 218
  - NIS 221
  - NIS+ 221
  - NTP 212
  - RDATE 214
  - remote logging 218
  - static shares 230
- shutting down 256
- unlocking console 247
- viewing
  - activity monitor 250
  - checkpoint analysis 253
  - port bonding 252
  - system log 251
- Temperature status 162
- Thin file server, defined 293
- Thresholds, setting
  - GUI 142
- Time
  - setting
    - GUI 61
    - telnet 211
  - synchronization
    - about 58
    - NTP 58
    - RDATE 58
    - setting up 59
    - setting, telnet 212
  - zone, setting
    - GUI 61
    - telnet 211

- Toolbar
  - defined 294
  - icons 10
  - using 10
- Trunking
  - see Bonding ports
- Trusted hosts
  - about 99
  - adding
    - GUI 99
    - telnet 244
  - deleting, telnet 245
  - editing 100
  - managing, telnet 244
  - removing 101
- Turning the server off 183
  - telnet 256

## U

- UID, defined 113
- Umask 114
- UNC, defined 294
- Unicode, defined 294
- Uninterruptible Power Supply
  - see UPS
- UNIX settings
  - name service lookup order 40
- Unix settings
  - mapping 102, 103
- Unix, mapping credentials 102
- Unlocking console 247
- Updating
  - ADS share containers 87
  - software 201
- UPS
  - defined 170
  - enabling monitoring 172
  - error messages 264
  - monitoring 170
- UPS subsystem errors 264
- URL
  - defined 294

Usage statistics  
file volumes 165  
mirroring 172  
network activity 166  
port activity 168  
system activity 166

## User

credentials  
defined 294  
mapping 101  
editing quotas 124  
groups  
about 93  
adding members, telnet 236  
configuring, telnet 235  
modifying privileges, telnet 237  
privileges 94  
removing members, telnet 237  
log facility 44  
quotas  
adding 120  
configuring 119  
default 119  
deleting 124  
editing 122  
root  
hard limits 119  
quotas 119  
soft limits 119

## Using

content panel 12  
GUI 9  
navigation panel 11  
online help 13  
system events panel 13  
toolbar 10

## V

Variations, configuration wizard 13

## Verify

DNS configuration 85  
name service lookup order 84

## Viewing

activity monitor, telnet 250  
backup  
job status 176  
tape status 176  
backup, log  
GUI 175  
checkpoint analysis, telnet 253  
controller information 172  
environmental status 161  
fan status 161  
file volume usage 165  
mirror statistics  
GUI 172  
network activity 166  
network routes 170  
port bonds, telnet 252  
port statistics 168  
power supply status 163  
system activity 166  
system log  
GUI 158  
telnet 251  
temperature status 162  
voltage status 164

Viewing status 157

Voltage status 164

## W

WAN, defined 294

Warning events, system log 160

Warning thresholds

about 142

setting

GUI 142

Web Administrator

connecting 7

content panel 12

GUI 9

logging in 8

navigating in 8

navigation panel 11

online help 13

system events panel 13

toolbar 10

Web browser, defined 294

## Windows

- autohome shares, about 117

- configuring SMB/CIFS 116

- domain

  - enabling 31

  - security 105

- mapping credentials 102

- security

  - models 31

- static shares, about 109

- workgroup

  - enabling 32

  - file directory security 104

  - security 113

## Windows Internet Naming Service

- see WINS

## WINS

- about 79

- defined 5, 294

- setting up 33

## Wizard

- running 13

- starting 14

- variations 13

## Workgroup

- defined 294

- security

  - enabling 32

Workstation, defined 294

WWW, defined 294