



Sun StorEdge™ 5210 NAS Appliance Administration Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 819-5376-10
January 2006, Revision A

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

Copyright 2006 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, Java, AnswerBook2, docs.sun.com, Sun StorEdge, 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.

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 2006 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, Java, AnswerBook2, docs.sun.com, Sun StorEdge, 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.

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.



Please
Recycle



Adobe PostScript

Contents

Preface xxiii

1. Introduction 1

Navigating in Web Administrator 1

 Toolbar 2

 Navigation Panel 3

 Folder Symbol Key 4

 Other Buttons 5

 Content Panel 6

 Status Panel 6

 Online Help 7

Running the Configuration Wizard 7

 ▼ To Start the Wizard 8

Where to Go From Here 9

2. Initial Network Configuration 11

Setting the Server Name 12

 ▼ To Set the Server Name 12

Configuring the Network Ports 12

 Port Locations 13

- ▼ To Configure Network Adapters 13
- Setting the Default Gateway Address 14
 - ▼ To Specify the Default Gateway Address 14
- Name Services 15
 - Configuring Windows Security 15
 - ▼ To Configure Windows Security 15
 - Setting Up WINS 17
 - ▼ To Set Up WINS 17
 - Setting Up DNS 17
 - ▼ To Set Up DNS 18
 - Setting Up NIS 19
 - ▼ To Set Up NIS 19
 - Setting Up NIS+ 20
 - ▼ To Set Up NIS+ 20
 - Configuring Name Services 21
 - ▼ To Set the Order for User, Group, Netgroup, and Host Lookup 21
- Setting Up Email Notification 22
 - ▼ To Set Up SMTP and Send Email Messages to the Recipients 22
- Setting Up Logging 23
 - ▼ To Set Up Remote and Local Logging 23
- Assigning the Language 24
 - ▼ To Assign the Language 25
- Backing Up Configuration Information 25
- Where to Go From Here 25

3. File System Setup and Management 27

- File System Concepts 27
 - RAID 27
 - RAID 0 (Not Supported) 28

RAID 5	28
LUN	29
Partition	29
File Volume	30
Segment	30
Creating the File System	30
Creating RAID Sets and LUNs	31
▼ To Add a New LUN	31
Designating a Drive as a Hot Spare	34
▼ To Designate a Drive as a Hot Spare	34
Creating a File Volume or a Segment	34
▼ To Create a File Volume or Segment Using the Create File Volume Panel	35
▼ To Create a File Volume or Segment Using the System Manager	36
Attaching Segments to a Primary File Volume	37
▼ To Attach a Segment Using the Attach Segments Panel	37
▼ To Attach a Segment Using the System Manager	38
Rebuilding a LUN	38
Removing a LUN	38
Removing a Hot Spare	39
File Volume and Segment Management	39
Editing File Volume Properties	40
▼ To Rename a Volume, Enable Checkpoints, Enable Quotas, or Edit Compliance Properties	40
Deleting File Volumes	41
▼ To Delete a File Volume or Segment	42
Viewing Volume Partitions	42
▼ To View Volume Partitions	42
Configuring iSCSI	43

Configuring an iSCSI Target	43
Configuring iSCSI Initiator Access	43
▼ To Create an iSCSI Access List	44
Creating iSCSI LUNs	45
▼ To Create an iSCSI LUN	46
iSCSI Target Discovery Methods	47
▼ To Configure an iSNS Server	48
Where to Go From Here	48
4. System Management	49
Setting the Administrator Password	49
▼ To Set the Administrator Password	49
Controlling the Time and Date	50
Setting Up Time Synchronization	50
▼ To Set Up Time Synchronization	51
Setting the Time and Date Manually	52
▼ To Set the Time and Date Manually	52
Using Anti-Virus Software	53
▼ To Enable Anti-Virus Protection	53
Virus Scanning	55
▼ To Delete Quarantined Files	56
5. Managing System Ports	57
Port Locations	57
About Alias IP Addresses	58
Port Bonding	58
Port Aggregation Bonds	58
High-Availability Bonds	59
Bonding Ports	59

- ▼ To Bond Ports 59
- 6. Active Directory Service and Authentication 61**
 - Supported Name Services 61
 - Active Directory Service 62
 - ▼ To Enable ADS 63
 - ▼ To Verify Name Service Lookup Order 64
 - ▼ To Verify DNS Configuration 65
 - ▼ To Publish Shares in ADS 65
 - ▼ To Update ADS Share Containers 66
 - ▼ To Remove Shares From ADS 66
 - Setting Up LDAP 67
 - ▼ To Enable LDAP Service 67
 - Changing Name Service Lookup Order 67
 - ▼ To Set the Order for User, Group, Netgroup, and Host Lookup 67
- 7. Group, Host, and File Directory Security 69**
 - Local Groups 69
 - Configuring Privileges for Local Groups 70
 - Ownership Assignment 71
 - Adding and Removing Group Members and Configuring Privileges 72
 - ▼ To Add or Remove a Member of a Group 72
 - Configuring Privileges 73
 - ▼ To Configure NT Privileges 73
 - Configuring Hosts 73
 - ▼ To Manually Add a Host 73
 - ▼ To Edit Host Information 74
 - ▼ To Remove a Host Mapping for a Particular Host 74
 - Mapping User and Group Credentials 75

UNIX Users and Groups	75
Windows Users and Groups	75
Credential Mapping	77
User Mapping	77
User Mapping Policy Settings	78
User Mapping Policy Example	78
Group Mapping	78
Group Mapping Policy Settings	79
Group Mapping Policy Example	79
Built-In Credential Mapping	80
▼ To Define the Mapping Policy	80
▼ To Map Windows Groups and Users to UNIX Groups and Users	81
Setting File Directory Security	82
Setting File Directory Security in Workgroup Mode	82
Setting File Directory Security in Domain Mode	82
▼ To Set Security	83
8. Shares, Quotas, and Exports	85
Shares	85
Static Shares	86
Configuring Static Shares	86
▼ To Add a New SMB Share	87
▼ To Edit an Existing SMB Share	89
▼ To Remove an SMB/CIFS Share	90
Configuring SMB/CIFS Clients	90
Windows 98, XP, and Windows NT 4.0	90
Windows 2000, XP, and 2003	90
DOS	91
Autohome Shares	91

- ▼ To Enable Autohome Shares 92
- Managing Quotas 92
 - Configuring User and Group Quotas 92
 - Hard and Soft Limits 92
 - ▼ To Enable Quotas for the File Volume 93
 - ▼ To Add a User or Group Quota 93
 - ▼ To Edit a User or Group Quota 94
 - ▼ To Delete a Quota 95
 - Configuring Directory Tree Quotas 95
 - ▼ To Create a Directory Tree With a DTQ 95
 - ▼ To Edit an Existing Directory Tree Quota 96
 - ▼ To Delete a Directory Tree Quota 97
 - Setting Up NFS Exports 97
 - ▼ To Create Exports 98
 - ▼ To Edit Exports 99
 - ▼ To Remove Exports 99
- 9. System Options 101**
 - Activating System Options 101
 - ▼ To Activate an Option 101
 - Sun StorEdge File Replicator 102
 - Sun StorEdge 5210 NAS Appliance Mirroring 103
 - Preparing for Mirroring 103
 - ▼ To Configure the Dedicated Network Ports 104
 - Configuring Mirrored File Volumes 104
 - Mirror Buffer 105
 - ▼ To Activate Sun StorEdge File Replicator on the Remote Server 105
 - ▼ To Add a File Volume 106
 - ▼ To Edit a Mirror 106

▼ To Correct a Cracked Mirror	107
Setting Warning Thresholds	107
▼ To Set Up the Threshold Alert	108
Breaking the Connection Between Mirror Servers	108
▼ To Break a Mirror Connection	109
Promoting a Mirrored File Volume	109
▼ To Promote a File Volume on the Mirror Server	109
Reestablishing a Mirror Connection	110
▼ To Reestablish a Mirror Connection	110
▼ To Break the Mirror Connection on the Active Server	111
▼ To Delete the Out-of-Date File Volume From Server 1	111
▼ To Mirror the Up-to-Date Volume From Server 2 to Server 1	111
Changing Volume Roles	112
▼ To Change Roles	112
Compliance Archiving Software	113
Enabling Compliance Archiving	113
Compliance With Mandatory Enforcement	114
Compliance With Advisory Enforcement	114
Compliance Auditing	115
File Size Limitations	115
Audit Log	116
Additional Compliance Archiving Features	117
10. Monitoring the System	119
SNMP Monitoring	120
▼ To Set Up SNMP	120
Viewing System Status	121
▼ To View System Status	121
System Logging	122

- ▼ To View the System Log 124
- System Events 124
- System Auditing 125
 - Audit Configuration 125
 - ▼ To Set Up System Auditing 125
 - Audit Log Files 126
 - Audited Events 126
 - Reading Audit Logs 126
- Environmental Status 127
 - ▼ To View Fan Status 127
 - ▼ To View Temperature Status 128
 - ▼ To View Power Supply Status 129
 - ▼ To View Voltage Status 130
- Usage Information 131
 - ▼ To View File Volume Usage 131
 - ▼ To View Network Activity 131
 - ▼ To View System Activity 132
 - ▼ To View Network (Port) Statistics 133
- Viewing Network Routes 134
 - About Routing 134
 - ▼ To Display Routes 134
- Monitoring System Components 135
 - UPS Monitoring 135
 - UPS Monitoring Capability 136
 - ▼ To Enable UPS Monitoring 136
 - Viewing Controller Information 136
 - ▼ To View Controller Vendor, Model, and Firmware Release 137
 - Viewing Mirroring Status 137

- ▼ To View Mirror Statistics 137
- Mirror Status States 138
- Viewing Backup Job Status 139
 - ▼ To View the Backup Log 139
 - ▼ To View Job Status 139
 - ▼ To View Tape Status 139

11. System Maintenance 141

- Setting Remote Access Options 141
 - ▼ To Set Remote Access Security 141
- Configuring FTP Access 142
 - ▼ To Set Up FTP Users 143
- Shutting Down the Server 143
 - ▼ To Shut Down, Halt, or Reboot the Server 143
- File Checkpoints 144
 - Creating File Checkpoints 144
 - ▼ To Create a New Checkpoint Manually 145
 - Scheduling File Checkpoints 145
 - ▼ To Add a Checkpoint to the Schedule 146
 - ▼ To Edit an Existing Checkpoint Schedule 147
 - ▼ To Remove a Schedule Line 147
 - ▼ To Rename a Checkpoint 147
 - ▼ To Remove a Checkpoint 148
 - Sharing File Checkpoints 148
 - ▼ To Share File Checkpoints 148
 - Accessing File Checkpoints 149
 - ▼ To Access a Checkpoint 149
- Setting Up NDMP for Backups 149
 - ▼ To Set Up NDMP 149

CATIA V4/V5 Character Translations	150
▼ To Enable CATIA Using the CLI	151
▼ To Enable CATIA Automatically on Reboot	151
Running a Head Cleaning	151
▼ To Run a Head Cleaning	151
Updating Sun StorEdge 5210 NAS Appliance Software	152
▼ To Update Software	152
A. Console Administration	155
Accessing the Console Administrator	156
▼ To Access Windows Telnet	156
▼ To Access the Command-Line Interface	156
Console Menu Basics	157
Basic Guidelines	157
Key Descriptions	157
Viewing the Main Menu	158
▼ To Use the Menu	158
Configuration Backup	158
▼ To Back Up the Configuration Information	158
System Management	159
▼ To Configure TCP/IP	159
▼ To Modify the Administrator Password	159
Controlling the Time and Date	160
▼ To Set the Time Zone, Time, and Date	160
▼ To Set Up NTP	161
▼ To Set Up the RDATE Server and Tolerance Window	162
Setting Up Anti-Virus Protection	162
▼ To Enable Anti-Virus Protection	162
Selecting a Language	163

- ▼ To Select a Language 164
- Managing Routes 164
 - ▼ To Manage Static Routes in the Local Network 164
- Name Services 164
 - ▼ To Set Up DNS, Dynamic DNS, syslogd, and Local Logging 165
 - ▼ To Enable NIS or NIS+ 167
 - ▼ To Set Up Lookup Orders 168
- Managing the Server File System 168
 - Configuring Drive Letters 168
 - ▼ To Manually Reassign a Drive Letter to a File Volume 169
 - ▼ To Create a New Disk Volume 169
 - ▼ To Rename a Partition 170
 - ▼ To Add an Extension Segment 170
 - ▼ To Delete a Disk Volume 171
- Managing Shares and Quotas 171
 - Setting Up SMB/CIFS Shares 171
 - ▼ To Set Up Shares 171
 - Setting Up SMB/CIFS Autohome Shares 172
 - ▼ To Enable Autohome Shares 173
 - ▼ To Define a Share 173
 - ▼ To Edit a Share 174
 - ▼ To Delete a Share 174
 - Setting Up Active Directory Service 174
 - ▼ To Enable ADS Service 174
 - Enabling and Disabling Quotas 175
 - ▼ To Enable or Disable Quotas 175
- Security 176
 - Configuring User Groups 176

- ▼ To Add a Group 176
- ▼ To Add a Member to a Group 176
- ▼ To Remove a Member From a Group 177
- Group Privileges 177
 - ▼ To Modify Local Group Privileges 177
- User and Group Maps 177
 - ▼ To Add a User Map 177
 - ▼ To Edit a User Map 178
 - ▼ To Remove a User Map 178
 - ▼ To Add a Group Map 178
 - ▼ To Edit a Group Map 179
 - ▼ To Remove a Group Map 179
- Mapping and Securable Objects 179
- Configuring the Host List 181
 - ▼ To Add a Host 181
 - ▼ To Edit an Existing Host 181
 - ▼ To Delete a Host 181
- Managing Trusted Hosts 181
 - ▼ To Designate a Trusted Host 181
 - ▼ To Delete a Trusted Host 182
- Managing Volume Access 182
 - ▼ To Manage Volume Access for NFS Clients 182
- Locking and Unlocking the Console 183
 - ▼ To Lock the Console 183
 - ▼ To Unlock the Console 183
- Mirroring File Volumes 183
 - Configuring Active and Mirror Servers 183
 - ▼ To Configure a New Active Server With a New Mirror Server 183

- ▼ To Configure an Existing Active Server With a New Mirror Server 184
- Configuring File Volumes 185
 - ▼ To Set Up a File Volume for Mirroring 185
 - ▼ To Mirror File Volumes 185
- Setting Warning Thresholds 186
 - ▼ To Set the Threshold Percentages at Which Warnings Are Issued 186
- Promoting a Mirrored File Volume 187
 - ▼ To Promote a File Volume on the Mirror System 187
- Reestablishing a Mirror 188
 - ▼ To Break the Mirror on Server 1 188
 - ▼ To Delete the Out-of-Date File Volume on Server 1 189
 - ▼ To Mirror the Up-to-Date File Volume on Server 2 Back to Server 1 189
 - ▼ To Change Roles 190
- Monitoring 190
 - Configuring SNMP 190
 - ▼ To Configure SNMP 190
 - Configuring Email Notification 190
 - ▼ To Configure Email Notification 191
 - Viewing System Information 191
 - ▼ To View Server Status 191
 - ▼ To View the System Log 192
 - ▼ To View Port Bonding 192
 - ▼ To View the Checkpoint Analysis 192
 - ▼ To View the Status of a Mirrored File Volume 192
 - ▼ To View Network Statistics for All Mirrored File Volumes 194
- System Maintenance 194
 - Configuring FTP Access 195

▼ To Set Up FTP Access	195
Mounting File Systems	196
Shutting Down the System	196
▼ To Shut Down the System	196
Scheduling File Checkpoints	197
▼ To Schedule Checkpoints	197
Configuring Backup	197
▼ To Set Up NDMP	198
Configuring the Compliance Archiving Software	198
▼ To Change the Default Retention Period	198
▼ To Allow Windows Clients to Use the Compliance Archiving Functionality	198
Configuring System Auditing	199
▼ To Configure System Auditing	199
B. Error Messages	201
About SysMon Error Notification	201
Sun StorEdge 5210 NAS Appliance Error Messages	201
UPS Subsystem Errors	202
File System Errors	204
RAID Subsystem Errors	204
IPMI Events	205
C. Compliance Archiving Software API	207
Compliance Features	207
WORM Files	208
Per-File Retention Periods	208
Administrative Lock-Down	208
Accessing Compliance Functionality	209
Compliance Volumes	209

WORM Files	209
File Retention Periods	211
Determining File Status	213
Behavior of UNIX System Calls	213
access(2)	213
chmod(2), fchmod(2)	213
chown(2), fchown(2)	214
link(2)	214
read(2), readv(2)	214
rename(2)	214
stat(2), fstat(2)	214
unlink(2)	215
utime(2), utimes(2)	215
write(2), writev(2)	215
Behavior of Windows Clients	215
Creating WORM Files	216
Metadata Restrictions on WORM Files	216
Setting Retention Periods	216
Caveats for Windows Clients	216
Other APIs	217
D. Sending a Diagnostic Email Message	219
Index	221

Figures

- FIGURE 1-1 Main Window 2
- FIGURE 1-2 Toolbar 2
- FIGURE 1-3 Navigation Panel 3

Tables

TABLE 1-1	Toolbar Icons	3
TABLE 1-2	Folder Symbols	4
TABLE 1-3	Other Buttons	5
TABLE 3-1	Add LUN Dialog Box Drive Status Indicators	33
TABLE 3-2	Add Hot Spare Drive Status Images	34
TABLE 3-3	Remove Hot Spare Drive Status Images	39
TABLE 7-1	Supported Privileges	71
TABLE 7-2	Default Group Privileges	71
TABLE 7-3	Fields in the SID	76
TABLE 8-1	Share Path Examples	86
TABLE 8-2	Umask Permission Examples	89
TABLE 9-1	Audit Log Format	116
TABLE 10-1	System Status Display	122
TABLE 10-2	System Event Icons	124
TABLE 10-3	Acceptable Voltage Ranges	130
TABLE 10-4	System and Network Devices	132
TABLE 11-1	CATIA Character Translation Table	150
TABLE A-1	Active Screen Keys	157
TABLE B-1	UPS Error Messages	202
TABLE B-2	File System Errors	204

TABLE B-3	RAID Error Messages	204
TABLE B-4	IPMI Error Messages	205
TABLE C-1	WORM File Metadata That Can and Cannot Be Modified	211

Preface

The *Sun StorEdge 5210 NAS Appliance Administration Guide* is a combined administrator's and user's guide for the Sun StorEdge™ 5210 NAS Appliance. This guide describes how to use the Web Administrator software to set up and monitor the system. It also includes instructions on using the command-line interface (CLI).

Before You Read This Book

Before reading this guide, you should already have installed and configured your system as described in the *Sun StorEdge 5210 NAS Appliance Hardware Installation, Configuration, and User Guide*.

How This Book Is Organized

This guide contains instructions for administering and using the Sun StorEdge 5310 NAS Appliance.

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

Chapter 2 describes basic network and file system configuration.

Chapter 3 describes redundant array of independent disks (RAID) system setup.

Chapter 4 describes management functions.

Chapter 5 describes port settings.

Chapter 6 describes naming conventions.

Chapter 7 describes security settings.

Chapter 8 describes shares, quotas, and exports.

Chapter 9 describes licensable software options.

Chapter 10 describes monitoring functions.

Chapter 11 describes maintenance functions.

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

Appendix B describes error messages that could appear.

Appendix C details the Compliance Archiving Software API.

Appendix D describes how to send a diagnostic email.

Typographic Conventions

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

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

Related Documentation

The documents listed as online are available at:

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

Title	Part Number	Format	Location
<i>Sun StorEdge 5210 and 5310 NAS Appliance and Gateway System Release Notes</i>	819-2857- <i>nn</i>	PDF	Online
<i>Sun StorEdge 5210 NAS Appliance Hardware Installation, Configuration, and User Guide</i>	817-6660- <i>nn</i>	PDF	Online
<i>Setting Up the Sun StorEdge 5210 NAS</i>	817-7430- <i>nn</i>	Printed	Shipping kit
<i>Attaching the Sun StorEdge 5210 NAS and Expansion Unit</i>	817-7513- <i>nn</i>	Printed	Shipping kit
<i>Sun StorEdge 5210 Expansion Unit Safety, Regulatory and Compliance Manual</i>	817-7515- <i>nn</i>	Printed	Shipping kit
<i>Sun StorEdge 5210 Expansion Unit Safety, Regulatory and Compliance Manual (Multi)</i>	819-1778- <i>nn</i>	PDF	Online

Documentation, Support, and Training

URL	Description
http://www.sun.com/documentation/	Download PDF and HTML documents, and order printed documents
http://www.sun.com/support/	Obtain technical support and download patches
http://www.sun.com/training/	Learn about Sun courses

Third-Party Web Sites

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

Sun Welcomes Your Comments

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

<http://www.sun.com/hwdocs/feedback>

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

Sun StorEdge 5210 NAS Appliance Administration Guide, part number 819-5376-10.

Introduction

The Web Administrator graphical user interface (GUI) for the Sun StorEdge 5210 NAS Appliance makes it easy to set security and network configurations, and to perform administrative tasks on Sun Microsystems innovative Sun StorEdge 5210 NAS Appliance.

Navigating in Web Administrator

The Web Administrator GUI 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.

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

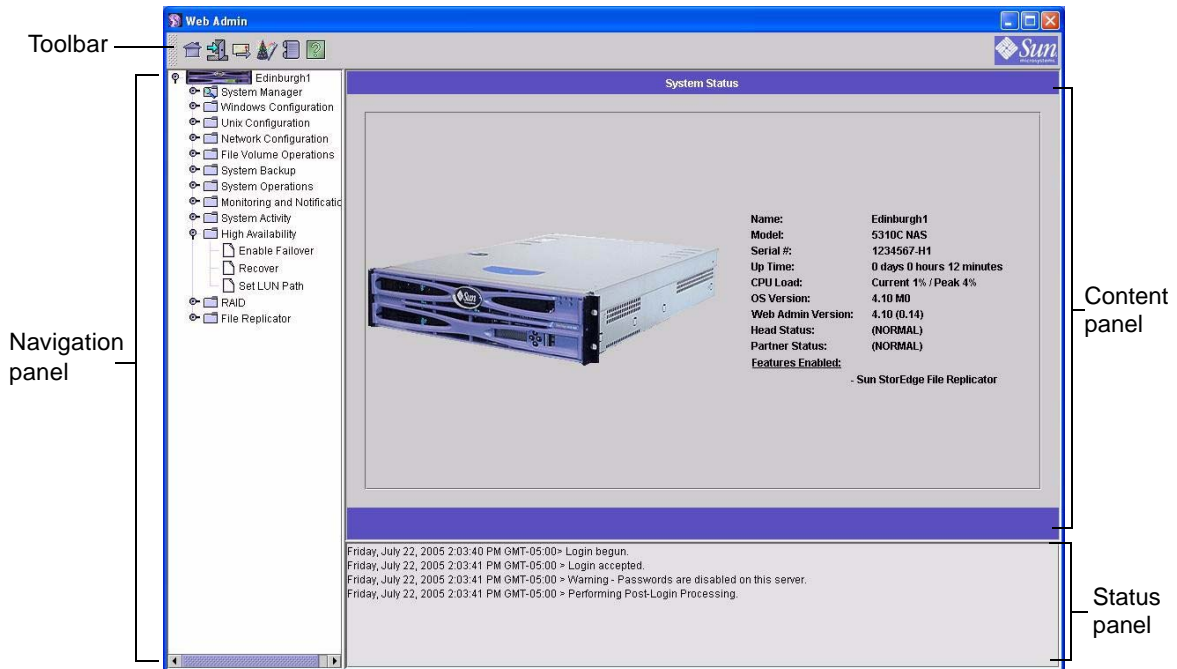


FIGURE 1-1 Main Window

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 1-2 Toolbar

The toolbar icons are shown in TABLE 1-1.

TABLE 1-1 Toolbar Icons

Button	Name	Action
	Home	View the home system status screen
	Log out	Log out
	Email	Send a diagnostic email
	Wizard	Run the configuration wizard
	System log	Access the system log
	Help	Access help

Navigation Panel

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

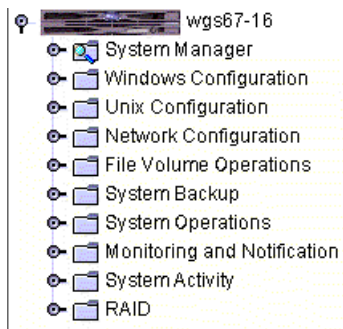


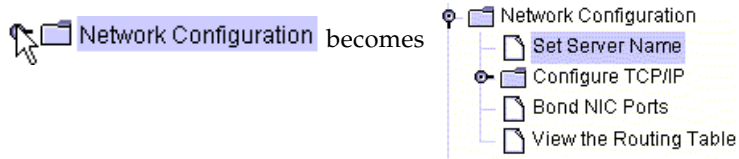




FIGURE 1-3 Navigation Panel

To open a folder, click the  symbol next to the folder, or double-click on the folder. The symbol changes to the  position. For example:











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

Folder Symbol Key

Throughout the Web Administrator folders are represented with symbols.

The folder symbols are shown in TABLE 1-2.

TABLE 1-2 Folder Symbols






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

Other Buttons

Certain screens in the Web Administrator contain other buttons.

Additional buttons are shown in TABLE 1-3.

TABLE 1-3 Other Buttons

Button	Name	Action
	Add	Add item
	Up	Move selected item down up
	Down	Move selected item down
	Trash	Delete selected item
	Edit	Edit selected item

Content Panel

This panel contains system general information.



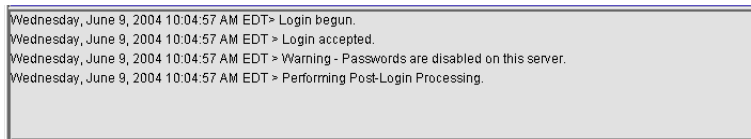
The screenshot shows a "System Status" window with a purple header. On the left is a photograph of a Sun StorEdge 5210 NAS appliance. On the right, the following system information is displayed:

Name:	Edinburgh1
Model:	5310C NAS
Serial #:	1234567-H1
Up Time:	4 days 4 hours 17 minutes
CPU Load:	Current 32% / Peak 33%
OS Version:	4.10 M0
Web Admin Version:	4.10 (0.12)
Head Status:	(NORMAL)
Partner Status:	(NORMAL)
Features Enabled:	- Sun StorEdge File Replicator

For details about system status, refer to "Viewing System Status" on page 121.

Status Panel

At the bottom of the Web Administrator window, the status 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.



The screenshot shows a status panel with a list of events:

- Wednesday, June 9, 2004 10:04:57 AM EDT > Login begun.
- Wednesday, June 9, 2004 10:04:57 AM EDT > Login accepted.
- Wednesday, June 9, 2004 10:04:57 AM EDT > Warning - Passwords are disabled on this server.
- Wednesday, June 9, 2004 10:04:57 AM EDT > Performing Post-Login Processing.

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

Online 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 Help 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 system. It helps you complete all of the steps necessary to establish communication between the system and your network. Once you complete the wizard, you still need to set up your file system and configure user access.

The configuration wizard offers several options. Some of these options are automatically determined by the system itself. Other options are determined by you, based on the network environment you are running. This guide cannot cover all of the 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 system. These variations are discussed in the appropriate locations within this guide.

There are three primary paths that you can choose for the wizard to take. These three paths are based on the network environment you are running. These three paths are as follows:

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

Select the path appropriate to your network environment.

▼ To Start the Wizard

1. To run the configuration wizard, click the Wizard button on the tool bar.

The wizard opens to an introductory page.

2. 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 Windows Internet Naming Service (WINS) (Windows environments and mixed environments)
6. Setting up the Domain Name Service (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

3. Confirm 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 system 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 configuring any LUNs, partitions, file volumes, and segments that you need to establish. See "File System Concepts" on page 27 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" covers the basic management functions.

Initial Network Configuration

This chapter describes configuring your system 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.

The following sections are included:

- "Setting the Server Name" on page 12
- "Configuring the Network Ports" on page 12
- "Setting the Default Gateway Address" on page 14
- "Name Services" on page 15
- "Setting Up Email Notification" on page 22
- "Setting Up Logging" on page 23
- "Assigning the Language" on page 24
- "Backing Up Configuration Information" on page 25
- "Where to Go From Here" on page 25

Setting the Server Name

You need to set up a server name that identifies the server on the network.

▼ To Set the Server Name

1. In the navigation panel, select **Network Configuration > Set Server Name**.
2. Enter the server name in the **Server Name** box.

This name identifies the system or this server unit, for 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 5210 NAS Appliance administrator.
The system includes this information in any diagnostic email messages sent. For more information about diagnostic email messages, refer to Appendix D.
4. Click **Apply** to save your settings.



Configuring the Network Ports

You can either enable DHCP or specify the IP address, netmask, broadcast for each network port through the Configure Network Adapters panel. You can also add alias IP addresses for each NIC port.

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 58.

Port Locations

The Sun StorEdge 5210 NAS Appliance identifies ports in a predefined order based on their type and their physical and logical location on the server. Refer to the *Sun StorEdge 5210 NAS 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 also shown in the *Sun StorEdge 5210 NAS Hardware Installation, Configuration, and User Guide*.

▼ To Configure Network Adapters

1. In the navigation panel, select **Network Configuration > Configure TCP/IP > Configure 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 system to dynamically acquire an IP address from the DHCP server. Clear this checkbox to manually enter a static IP address and netmask. If you do not enable DHCP, the netmask is still disabled if the port is a member of an aggregate port. See "Port Bonding" on page 58 for more information on creating and setting up aggregate ports.

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 58 for more information on creating port bonds.) Independent ports are labeled PORT x and port bonds are labeled BOND x .

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.

Roles	Description
Primary	Identifies an active network port.
Independent	Identifies an active network port used for purposes other than serving data, such as backup.
Mirror	Shows that the port connects this server to another server to mirror file volumes.

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

For more details about port roles, refer to "Port Locations" on page 57.

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

You can have up to nine aliases. To remove an alias from the list, select it and click the Trash button. 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. You must specify the default gateway address for the system.

▼ To Specify the Default Gateway Address

1. In the navigation panel, select **Network Configuration > Configure TCP/IP > Set Gateway Address**.
2. Enter the gateway address in the **Gateway** text box.
3. Click **Apply** to save your settings.

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 6, "Active Directory Service and Authentication" on page 61.

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

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.

 - 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 must be 16 characters or fewer.
- 3. To enable Windows workgroup security, select the Workgroup option, and enter the name of the workgroup in the Name field.**

The workgroup name must conform to the 15-character NetBIOS limitation.
- 4. (Optional) In the Comments field, enter a description of the Sun StorEdge 5210 NAS Appliance system.**
- 5. To enable ADS, click the Enable ADS checkbox.**

For more detail about ADS, refer to "Active Directory Service" on page 62.

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

a. In the Domain field, enter the Windows Domain in which ADS is running.

The system must belong to this domain.

b. In the User Name field, enter the user name of a Windows 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 the same password can be reused. For more information, refer to the Microsoft Support Services Web site, Article Q248808.

c. In the Password field, enter the Windows administrative user's password.

d. In the Container field, enter the ADS path location of the Windows administrative user in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation.

For more information, see "Active Directory Service" on page 62.

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

e. If the ADS domain uses sites, enter the appropriate site name in the Site field. Otherwise, leave the Site field blank. If specified, the Site will be included when selecting a domain controller.

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 uppercase 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 system 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.

2. To enable WINS, click the Enable WINS checkbox.

Checking this box makes the system 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 system consults the secondary WINS server.

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

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

6. Click Apply to save your settings.

Setting Up DNS

The Domain Name Service(DNS) resolves host names to IP addresses for your Sun StorEdge 5210 NAS Appliance.

Note – If you are using DNS without Dynamic DNS, add the 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**.
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, and then click the Add button to add the server to the Server list**.

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

The system first queries the DNS server at the top of the server list for domain name resolution. If that server cannot resolve the request, the query goes to the next server on the list.

5. To rearrange the search order of the DNS servers in the list, click the server you want to move and click the **Up or Down button**.

To remove a server from the list, select the server IP address and click the **Trash button**.

6. Select the **Enable Dynamic DNS** checkbox to let a **Dynamic DNS client add the Sun StorEdge 5210 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 15. If you enable Dynamic DNS by selecting this checkbox, nonsecure dynamic updates occur automatically if they are allowed by the DNS server.

7. To enable secure Dynamic DNS updates, provide the following information. This information is not required for nonsecure updates.

- a. In the **DynDNS User Name** field, enter the user name of a Windows 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 15.

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.

You use the **Set Up NIS** panel 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**.
2. Select the **Enable NIS** checkbox.
Enabling NIS configures the system 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. Enter the frequency rate, in minutes, at which you want NIS information to be refreshed. The default is set to 5 minutes.
6. Select the **Use Broadcast** checkbox to automatically acquire the NIS server IP address.
7. Select the **Update Hosts** checkbox to download host information from the NIS server to the system.
8. Select the **Update Users** checkbox to download user information from the NIS server to the system.
9. Select the **Update Groups** checkbox to download group information from the NIS server to the system.
10. Select the **Update Netgroups** checkbox to download netgroup information from the NIS server to the system.
11. Click **Apply** to save your changes.

Setting Up NIS+

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

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

▼ To Set Up NIS+

1. **For the Sun StorEdge 5210 NAS Appliance to function correctly in an NIS+ environment, you must add it 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 5210 NAS Appliance and *DOMAIN* is the name of the NIS+ domain that the Sun StorEdge 5210 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 5210 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. **At the prompt, enter a password.**

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

2. **From a remote client, open a web browser window to the system and log in to Web Administrator.**
3. **In the navigation panel, select UNIX Configuration > Set Up NIS+.**
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 system 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 20.

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, the system first searches **eng.sun.com.** then **sun.com.**, and so on, when resolving names. Conversely, if you specify a search path like **sun.com.**, the system searches only the domain **sun.com** when resolving names.

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.
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. Arrange the order of lookup services in the Services Selected box by selecting each service and clicking the Up and Down buttons to move it up or down. The service at the top of the list is used first in user lookup.

- e. If you want to remove a service from user lookup, select it and click the < button.
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, it sends a notification email message.

In order to ensure name resolution, you must have either set up the SMTP server host name in the **Configure Hosts** panel (see "Configuring Hosts" on page 73) or set up DNS (see "Setting Up DNS" on page 17).

▼ To Set Up SMTP and Send Email Messages to the Recipients

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

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

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



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

▼ To Set Up Remote and Local Logging

1. **In the navigation panel, select Monitoring and Notification > View System Events > Set Up Logging.**
2. **Select the Enable Remote Syslogd box.**
3. **In the Server field, enter the DNS host name if you have configured the DNS settings. Otherwise, enter the IP address. This is where the system log is sent.**
4. **Select the appropriate facility.**

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

Note – All messages sent to the syslogd server will have this facility value.

The possible facility values in the Set Up Remote Logging panel are as follows:

Facility	Description
Kern	Messages generated by the kernel. These cannot be generated by any user processes.
User	Messages generated by random user processes. This is the default facility identifier if none is specified.
Mail	The mail system.
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 to log by placing a check mark on the type of event (see “System Events” on page 124).**
6. **Check the Enable Local Log option to maintain a local log file.**
7. **Enter the log file’s path (the directory on the system where you want to store the log file) and file name in the 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 operating system supports Unicode, which enables you to set the local language for NFS and CIFS. Ordinarily, you assign the language when you run the wizard during initial system setup. However, if you need to reset the language at a later time, you can set it manually.

▼ To Assign the Language

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

Backing Up Configuration Information

After you have completed system configuration, you should back up the configuration information in the event of a system failure. Refer to "Configuration Backup" on page 158 for details on backing up configuration information.

Where to Go From Here

At this point, your system is in full communication with the network. However, before your users can begin storing data, you must set up the file system and establish user access rights. The next chapter, "File System Setup and Management" on page 27, describes the setup of a file system.

To set up quotas, shares, exports, or other access controls, see "Shares, Quotas, and Exports" on page 85 for detailed instructions.

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

File System Setup and Management

This chapter covers file system concepts, setup, and management for the Sun StorEdge 5210 NAS Appliance .

This chapter includes the following topics:

- "File System Concepts" on page 27
- "Creating the File System" on page 30
- "Creating a File Volume or a Segment" on page 34
- "Rebuilding a LUN" on page 38
- "File Volume and Segment Management" on page 39
- "Configuring iSCSI" on page 43
- "Where to Go From Here" on page 48

File System Concepts

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

RAID

RAID, redundant array of independent disks, 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. The Sun StorEdge 5210 NAS Appliance supports RAID 5 only.

RAID 0 (Not Supported)

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

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

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.

RAID 5 uses striping and *parity* information. Parity information is data created by combining the bits in the information to be stored and creating a small amount of data from which the rest of the information can be extracted. In other words, the parity information repeats the original data in such a way that if part of the original is lost, combining the remainder of the original and the parity data reproduces the complete original. The parity information is not stored on a specific drive. Instead, a different drive in the stripe set is used for parity protection for different regions of the RAID 5 set.

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

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



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

LUN

A logical unit number (LUN) identifies the logical representation of a physical or virtual device. In the Sun StorEdge 5210 NAS Appliance there is a one-to-one correspondence between RAID sets and LUNs. However, the system manages LUNs as independent entities and treats the LUN as a single storage volume.

By treating LUNs this way, the Sun StorEdge 5210 NAS Appliance greatly simplifies the process of establishing a file system. The space on the RAID set is accessed independently of the physical drive limits through the LUN.

Management of the storage resources is accomplished through the LUN, with little direct management of the RAID sets themselves. See "Creating RAID Sets and LUNs" on page 31 for directions and more information on setting up both RAID sets and LUNs.

Partition

Partitions are sections on a LUN and provide a way to subdivide the total space available within a LUN. The Sun StorEdge 5210 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 30). The segment is essentially another file volume with special characteristics. When you add a segment to an existing volume, the two become inseparable and the only thing the user sees is more space in the volume. The flexibility of this system enables you to create a file volume and then to expand it as needed without disturbing your users and without forcing them to spread their data over several volumes.

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

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 gigabyte in size. To create a larger file volume, you can create and attach up to 63 segments (see "Segment" on page 30) 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. They can be attached to an existing file volume at any time. Attaching a segment increases the original file volume's total capacity. Each segment must be created independently and then attached to a file volume. Once attached to a file volume, the volume and the segment are inseparable.

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

Creating the File System

If you are configuring a Sun StorEdge 5210 NAS Appliance, refer to the sections "Creating RAID Sets and LUNs" on page 31 and "Designating a Drive as a Hot Spare" on page 34.

Creating RAID Sets and LUNs

The Sun StorEdge 5210 NAS Appliance combines the creation and definition of the RAID set into the definition of the LUN. (See "File System Concepts" on page 27 for more information.) In effect, you create both objects simultaneously. The Sun StorEdge 5210 NAS Appliance lets you choose the basic structure of the RAID set and define the LUN, automating the many tasks usually associated with defining a RAID set.

The Sun StorEdge 5210 NAS Appliance also automates the definition of partitions. Partitions are automatically defined when you create a LUN. Initially, the Sun StorEdge 5210 NAS Appliance has two hot spare drives assigned and at least two default LUNs.

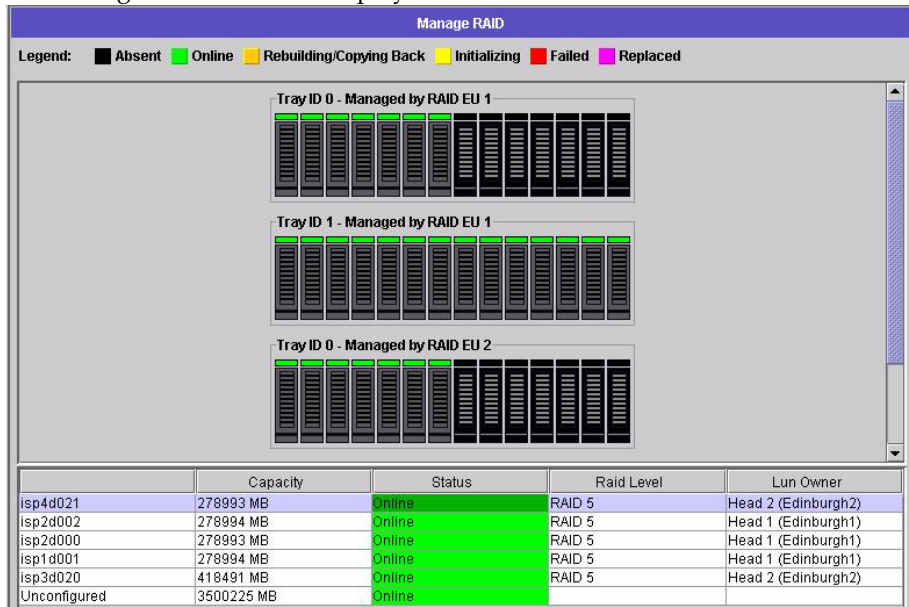
RAID sets and LUNs are created simultaneously in the Sun StorEdge 5210 NAS Appliance, simplifying the process of establishing both.

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

▼ To Add a New LUN

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

The Manage RAID Panel is displayed.



The screenshot shows the "Manage RAID" interface. At the top, there is a legend with color-coded boxes: Absent (black), Online (green), Rebuilding/Copying Back (yellow), Initializing (orange), Failed (red), and Replaced (magenta). Below the legend, there are three RAID trays:

- Tray ID 0 - Managed by RAID EU 1
- Tray ID 1 - Managed by RAID EU 1
- Tray ID 0 - Managed by RAID EU 2

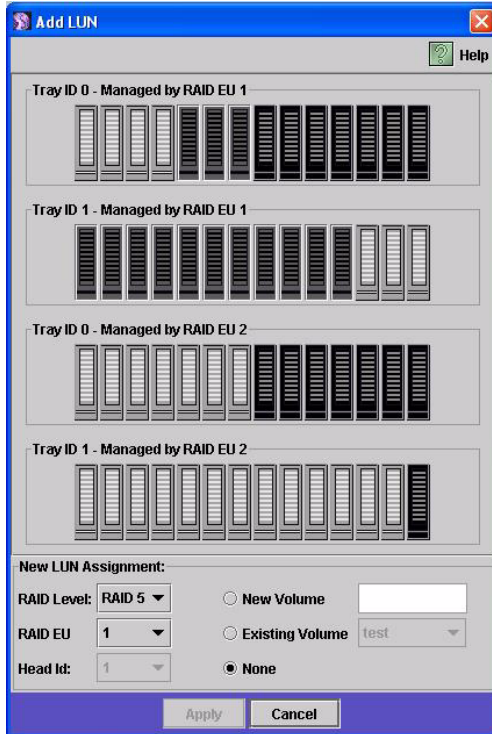
Each tray contains a row of 10 drive indicators. Below the trays is a table with the following data:

	Capacity	Status	Raid Level	Lun Owner
isp4d021	278993 MB	Online	RAID 5	Head 2 (Edinburgh2)
isp2d002	278994 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp2d000	278993 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp1d001	278994 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp3d020	418481 MB	Online	RAID 5	Head 2 (Edinburgh2)
Unconfigured	3500225 MB	Online		

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

2. Click **Add LUN**.

The Add LUN window is displayed.






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

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

You must select at least three drives. The drive images show the status of each drive.

TABLE 3-1 Add LUN Dialog Box Drive Status Indicators

Drive	Indication
	The drive in this slot is available for LUN membership.
	The drive in this slot has been selected for LUN membership.
	No drive is present in this slot.

5. Choose one of the following volume options.

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

6. Click Apply to add the new LUN.

Allow several hours for the system to add the LUN.

Designating a Drive as a Hot Spare

You can configure a drive as a hot spare for the Sun StorEdge 5210 NAS Appliance.




▼ To Designate a Drive as a Hot Spare

1. In the navigation panel, select RAID > Manage RAID.
2. Click the Add HS button at the bottom of the screen.
3. Select the drive you want by clicking the drive image.

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

The drive images show the status of each drive.

TABLE 3-2 Add Hot Spare Drive Status Images

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

4. Click Apply to add the new hot spare.

Creating a File Volume or a Segment

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

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

▼ To Create a File Volume or Segment Using the Create File Volume Panel

1. In the navigation panel, select **File Volume Operations > Create File Volumes**.
2. If you have recently added new disks to the live system without performing a reboot, click the **Scan For New Disks** button.
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** pull-down menu will automatically increment when the file volume is created.

4. Type in the name of the new volume or segment in the **Name** field.
Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).
5. Select whether the size of the file volume is reported in **MB (megabytes)** or **GB (gigabytes)** by clicking on the pull-down menu.
6. Type in the file volume size in whole numbers.
The total space available is shown directly beneath this field.
7. Select the file volume type (**Primary or Segment**).
8. If you have the **Compliance Archiving** software installed and you want to create a compliance-enabled volume, click **Enable** in the **Compliance** section. Then specify the type of compliance enforcement that is needed.
 - If you select **Mandatory Enforcement**, the default retention time will be permanent. Administrative override is not permitted.



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

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

Note – Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See “Managing Trusted Hosts” on page 181.

For more information, see "Compliance Archiving Software" on page 113.

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

▼ To Create a File Volume or Segment Using the System Manager

1. **Right-click System Manager in the Navigation Panel.**
2. **Choose Create Volume or Create Segment from the pop-up menu to open the desired 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** pull-down menu will automatically increment when the file volume is created.

4. **Type in the name of the new volume or segment in the Name field.**
Valid characters include alphanumeric (a–z, A–Z, 0–9) characters. The name must be 12 characters or fewer and must begin with an alphabetical character (a–z, A–Z).
5. **Select whether the size of the file volume is reported in MB (megabytes) or GB (gigabytes) by clicking on the pull-down menu.**
6. **Type in the file volume size in whole numbers.**
The total space available is shown directly beneath this field.
7. **Select the file volume type (Primary or Segment).**
8. **If you have the Compliance Archiving software installed and you want to create a compliance-enabled volume, click Enable in the Compliance section. Then specify the type of compliance enforcement that is needed.**
 - In you select Mandatory Enforcement, the default retention time will be permanent. Administrative override is not permitted.



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

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

Note – Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See “Managing Trusted Hosts” on page 181.

For more information, see "Compliance Archiving Software" on page 113.

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 the size of the volume. The segment becomes permanently associated with the volume and cannot be removed. You must create a segment before you can attach it to a volume. Refer to "Creating a File Volume or a Segment" on page 34 for instructions.



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

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

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



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

▼ To Attach a Segment Using the Attach Segments Panel

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

▼ To 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 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.**
5. **Repeat Steps 3 and 4 to attach more segments.**

Rebuilding a LUN

If one of the drives in a LUN fails, the LED on that drive turns steady amber, indicating it is waiting to be replaced with a new drive.

If a hot spare drive is available, the RAID set associated with the failed drive will be rebuilt using that hot spare. All drives associated with the rebuild will have LEDs blinking green and should not be removed during the rebuilding process. Rebuilding can take several hours to complete. When you replace the faulty drive, you must manually assign the new drive as the hot-spare.

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 for information on replacing a failed drive. The RAID controller will automatically rebuild the LUN, but only the new drive will blink amber, the other drives will blink green.

Removing a LUN

When removing a LUN, you can only remove the most recently created LUN per controller. The Remove LUN button will be enabled for those LUNs that can be removed.

To remove a LUN:

1. **In the navigation panel, select RAID > Manage RAID.**
2. **Click Remove LUN.**

The system automatically selects the drives belonging to the LUN you are removing. You can only remove the most recently added LUN.



Caution – When you select Yes, all data on the LUN will be destroyed.

3. Click **Yes** to remove the LUN.





Removing a Hot Spare

To remove hot spare status from a drive in the RAID array:

1. In the navigation panel, select **RAID > Manage RAID**.
2. Select the hot spare to be removed by clicking the drive image. If there is only one hot spare, it is automatically selected.

The drive images show the status of each drive as follows:

TABLE 3-3 Remove Hot Spare Drive Status Images

Drive	Indication
	The drive in this slot is a hot spare.
	The drive in this slot has been selected for removal.
	The drive in this slot cannot be selected because it is not a hot-spare
	No drive is present in this slot.

3. Click **Remove HS**.
4. Click **Yes** to remove the hot spare.

File Volume and Segment Management

File system management tasks include the following:

- "Editing File Volume Properties" on page 40
- "Deleting File Volumes" on page 41
- "Viewing Volume Partitions" on page 42

Editing File Volume Properties

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

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

▼ To Rename a Volume, Enable Checkpoints, Enable Quotas, or Edit Compliance Properties

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

2. Select the name of the volume you want to change from the **Volumes** list.

3. Enter the volume's new name (if applicable) in the **New Name** field.

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

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

Option	Description
Enable Checkpoints	Select this checkbox to create checkpoints for the file volume. Checkpoints are enabled by default when you create a file volume.
Enable Quotas	Select this checkbox to enable quotas for the selected volume. Quotas are disabled by default when you create a file volume.
Enable Attic	Select this checkbox to temporarily save deleted files in the <code>.attic\$</code> directory located at the root of each volume. By default, this option is enabled. In rare cases on very busy file systems, the <code>.attic\$</code> 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 <code>.attic\$</code> directory by deselecting this checkbox.

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



Caution – For compliance-enabled volumes with mandatory enforcement, the default retention time is “Permanent.” For compliance-enabled volumes with advisory enforcement, the default retention time is zero days. If you want to set a different default retention time, you must specify the new retention period *before* you begin using the volume.



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

For more information, see "Compliance Archiving Software" on page 113.

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

6. Click Apply to save your changes.

Deleting File Volumes

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 41.)

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 "To Remove a Checkpoint" on page 148 for instructions on removing checkpoints.

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

▼ To Delete a File Volume or Segment

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

Viewing Volume Partitions

The View Volume Partitions panel is a read-only display of the LUNs defined for the Sun StorEdge 5210 NAS Appliance.

▼ To View Volume Partitions

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

The following information is shown for the selected volume.

Field	Description
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.

Configuring iSCSI

You can configure the system to use the iSCSI (Internet Small Computer Systems Interface) protocol to transport data from host applications to the Sun StorEdge 5210 NAS Appliance storage. iSCSI transports SCSI commands, data, and status over a network file system Transmission Control Protocol/Internet Protocol (TCP/IP) network. When you enable iSCSI, host applications can store data on the Sun StorEdge 5210 NAS Appliance.

In an iSCSI environment, the Sun StorEdge 5210 NAS Appliance acts as the iSCSI target for an iSCSI initiator client. Each iSCSI initiator and target pair has a unique, permanent identifier. The iSCSI initiator identifier is generated by iSCSI software on the host. The iSCSI target supports both EUI (Enterprise Unique Identifier) and IQN (iSCSI Qualified Name) identifiers.

Configuring an iSCSI Target

Configuring an iSCSI target to connect to and access an iSCSI target LUN requires the following steps:

1. Configuring the iSCSI initiator client (see the documentation provided with the iSCSI initiator software)
2. Creating an access list to enable iSCSI initiator access to the target
3. Creating a logical unit number (LUN) and assigning iSCSI initiator access to the LUN
4. Configuring the iSCSI target and initiator discovery method

The iSCSI target implemented on the Sun StorEdge 5210 NAS Appliance is based on iSCSI RFC 3720 developed by the Internet Engineering Task Force (IETF). The supported protocol features include header digest, initiator Challenge Handshake Authentication Protocol (CHAP), and error recovery level 0.

Configuring iSCSI Initiator Access

You can define which iSCSI initiators can access a LUN by creating an iSCSI access list. An access list can include one or more iSCSI initiators and, optionally, a CHAP initiator and password. CHAP ensures that the data is sent from an authentic iSCSI initiator.



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

▼ To Create an iSCSI Access List

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

The Add iSCSI Access dialog box is displayed.

The screenshot shows a dialog box titled "Add iSCSI Access". It features a blue header bar with the title and a close button. Below the header, there is a "Help" button. The main area contains four input fields: "* Name:", "CHAP Initiator Name:", "CHAP Initiator Password:", and "Initiator IQN Name:". Below these fields is a list box labeled "Initiator IQN List" with a trash icon. At the bottom, there are "Apply" and "Cancel" buttons. A "* Required Fields" note is located at the bottom left of the dialog.

3. Specify the following information:

Field	Description
Name	Enter a name for the access list. The name must consist of one or more characters and can contain alphanumeric characters (a-z, A-Z, 0-9), period (.), hyphen (-), or colon (:). For example, <code>iscsiwinxp</code> is a valid access list name.
CHAP Initiator Name	Enter the full name of the CHAP initiator that is configured by the iSCSI initiator software. The default CHAP initiator name for a Windows iSCSI client is: <code>iqn.1991-05.com.microsoft:iscsi-winxp</code> If you leave this field blank, CHAP authorization will not be required. Refer to the iSCSI initiator documentation for more information.
CHAP Initiator Password	If you provided a CHAP initiator name, enter the CHAP initiator password.
Initiator IQN Name	Enter an initiator IQN name and click the Add button to add an initiator to the list. If you leave this field blank, any initiator can access the target. The name can consist of one or more characters and can contain alphanumeric characters (a-z, A-Z, 0-9), period (.), hyphen (-), or colon (:). To remove an initiator IQN from the list, select the name and click the Trash button.

4. Click Apply to save the settings.

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

Creating iSCSI LUNs

Before creating a LUN, you should decide whether you want the LUN to be sparse or non-sparse. As a general rule, you should use non-sparse LUNs whenever sufficient storage is available.

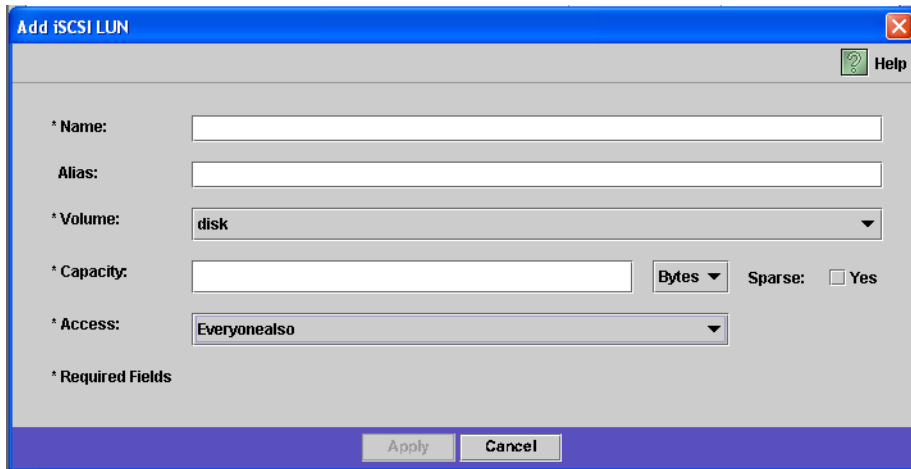
iSCSI sparse LUNs are not useful in all situations. If you create sparse LUNs, disk space is not allocated prior to use. Sparse LUNs are useful when you expect that several LUNs will be created that will not use their full capacity. For example, when you expect that five iSCSI LUNs of 100 GB each will use only 55% of their capacity, you can create them all on a volume that can hold $5 * 100 * .55 = 275$ GB, plus 50 GB for growth, for a total of 325 GB.

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

▼ To Create an iSCSI LUN

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

The Add iSCSI LUN dialog box is displayed.



The screenshot shows the "Add iSCSI LUN" dialog box. It features a blue title bar with the text "Add iSCSI LUN" and a red close button. Below the title bar is a grey area with a "Help" icon and text. The main area contains several fields: "* Name:" with a text input; "Alias:" with a text input; "* Volume:" with a dropdown menu showing "disk"; "* Capacity:" with a text input, a "Bytes" dropdown, and a "Sparse:" checkbox with "Yes" selected; "* Access:" with a dropdown menu showing "Everyonealso". At the bottom, there is a "* Required Fields" label and two buttons: "Apply" and "Cancel".

3. Specify the following information:

Field	Description
Name	<p>Enter a name for the iSCSI LUN. The name can consist of one or more characters and can contain alphanumeric characters (a–z, A–Z, 0–9), a period (.), hyphen (-), or colon (:).</p> <p>The target name you provide will be prefixed with the full IQN name using the following naming convention:</p> <pre>iqn.1986-03.com.sun:01:mac-address.timestamp.user-specified-name</pre> <p>For example, if you enter the name <code>lun1</code>, the full name of the iSCSI target LUN is as follows:</p> <pre>iqn.1986-03.com.sun:01:mac-address.timestamp.lun1</pre> <p>Note: The timestamp is a hex number representing the number of seconds after 1/1/1970.</p>
Alias	(Optional) Enter a brief description about the target.
Volume	Select the name of the volume where the iSCSI LUN is to be created.
Capacity	Specify the maximum size for the LUN in bytes, KB, MB, or GB.
Sparse	<p>Select the Yes box if you want to create a sparse LUN. A sparse LUN sets the file size attribute to the specified capacity, but the disk blocks are not allocated until data is written to the disk. See “Creating iSCSI LUNs” on page 45 for more information.</p> <p>If you create a non-sparse LUN, disk blocks will be allocated based on the capacity of the LUN you are creating. When creating non-sparse iSCSI LUNs, allow approximately 10% extra space on the volume for file system metadata. For example, a 100-GB iSCSI LUN should reside on a 110-GB volume to allow non-sparse LUN creation.</p> <p>For more information about deciding to use sparse or non-sparse LUNs see “Creating iSCSI LUNs” on page 45.</p>
Access	Select the access list (previously created) for this LUN.

4. Click Apply to save the settings.

iSCSI Target Discovery Methods

You can configure how an iSCSI initiator finds an iSCSI target by using one of the following methods:

- Static configuration – Manually add the iSCSI target name or IP address to the iSCSI initiator host. Refer to the documentation provided with your iSCSI initiator software for details.

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

▼ To Configure an iSNS Server

To enable an iSNS server, you specify the IP address or DNS name of the iSNS server. The iSNS client interoperates with any standard iSNS server implementation, such as Microsoft iSNS Server 3.0.

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

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

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

Where to Go From Here

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

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

System Management

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

System management functions include the following:

- "Setting the Administrator Password" on page 49
- "Controlling the Time and Date" on page 50
- "Using Anti-Virus Software" on page 53

Setting the Administrator Password

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

▼ To Set the Administrator Password

1. In the navigation panel, select **System Operations > Set Administrator Password**.
2. Enter the old password (if any) in the **Old Password** field.
If there is no password, leave this field blank.
3. Enter the new password in the **New Password** field.

The password must be at least 1 and no more than 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 system is essential for controlling file management. This section describes the functions available to maintain the correct time and date.

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

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



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

Setting Up Time Synchronization

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

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

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

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

▼ To Set Up Time Synchronization

1. In the navigation panel, select System Operations > Set Up Time Synchronization.

2. Choose one of the following three options:

- Manual Synchronization – Select this option if you do not want to use either NTP or RDATE time synchronization.
- NTP Synchronization – 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 system will poll for the current time.
 - Auth Type – Authentication support allows the system to verify that the server is known and trusted by using a key and key identifier. The NTP server and the system 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 system 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 system 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 – The name or IP address of the RDATE server.
 - Tolerance – The maximum tolerance allowed for the time received from the RDATE server, from 0 to 3600 seconds. If the system time is different than the RDATE server time by less than this number of seconds (+ or –), the system time is synchronized with the RDATE server time. If there is a larger discrepancy, the system 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

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

▼ To Set the Time and Date Manually

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

8. **Click Apply to save your time and date settings.**

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

Using Anti-Virus Software

Anti-virus protection is available through Internet Content Adaptation Protocol (ICAP) connections to “scan engines” you have installed on your network. When you enable anti-virus protection on the Sun StorEdge 5210 NAS Appliance, the system becomes a client of the anti-virus engine you are using on your network.

Note – If you configure virus protection on your system, you must have at least one scan engine operational at all times. If you do not, Microsoft Windows clients may be denied access.

▼ To Enable Anti-Virus Protection

1. In the navigation panel, select **Configure Anti Virus**.
2. Select the **Enable Anti Virus** checkbox.

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

3. Select the scan mode.

Scan Mode	Description
Scanning Suspended	Temporarily suspends anti-virus protection. Note: Anti-virus protection is not in effect when this option is selected.
Scan after Modify	Select this option to perform a scan after any files have been modified. This option offers a compromise between performance and thoroughness of virus protection, enabling fast read access but virus protection only as current as the time of file modification. Later access to the file will not take into account that virus definitions may have changed.
Scan all Access	Performs a scan after any access of the system. This option offers the most thorough virus protection, allowing access only to data that has been scanned with the latest virus definitions.

4. Specify the TCP/IP address of the scan engine you want to use.
5. Specify the TCP/IP port number on which the ICAP server listens for connections; this is typically port 1344.
6. Specify the maximum number of concurrent file scan operations that your system will dispatch to the scan engine; this is typically 2.

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

Specification	Description	Format
File Types Included	Leave blank to include all. Otherwise, select each file type extension to be included in scanning.	Three or fewer characters. Can use ? for wildcard matching.
File Types Excluded	Select each file type extension to be excluded from scanning.	Three or fewer characters. Can use ? for wildcard matching.
Exempt Clients	Name or IP address of each client exempt from scanning.	
Exempt Groups	Name of each Windows/NT or Windows Active Directory group (not UNIX groups) exempt from scanning.	Can include spaces.
Exempt Shares	Name of each Common Internet File System (CIFS) share exempt from scanning. Note: Administrative shares (X\$) are always exempt from scanning.	

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

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

8. Click **Apply** to save your settings.

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

Virus Scanning

During normal operation, users at CIFS clients may observe a short delay when virus scanning occurs, particularly with the Scan all Access option selected.

When a virus is detected, an entry is added to the system log that records the name of the infected file, the name of the virus, and the disposition that was selected for the file. In most cases, the disposition is to quarantine the infected file and deny access to the CIFS client. Quarantined files are visible in the /quarantine directory at the root of the file system containing the infected file. In order to avoid name conflicts in the /quarantine directory, files are named based on an internal

number: *NNNNNN.vir* is a hard link to the infected file, and *NNNNNN.log* is a text file containing the original name of the infected file, and the details of the infections detected.

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

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

▼ To Delete Quarantined Files

1. **Determine the original name from either the system log or the *NNNNNN.log* file in the `quarantine` directory, and delete that file if it still exists.**
2. **Examine the quarantine directory for the two files *NNNNNN.vir* and *NNNNNN.log* corresponding to the infected file, and delete those.**

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.

This chapter includes the following topics:

- “Port Locations” on page 57
- “About Alias IP Addresses” on page 58
- “Port Bonding” on page 58

Port Locations

The Sun StorEdge 5210 NAS Appliance identify ports in a predefined order based on their type and their physical and logical location on the server. Refer to the *Sun StorEdge 5210 NAS Appliance Hardware Installation, Configuration, and User Guide* to identify the port locations for your system.

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

- Primary – The port role of Primary identifies an active network port. At least one port must be assigned a primary role.
- 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. 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 102.

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.

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 of greater bandwidth. High-availability bonding combines two or more ports to provide NIC port failover services or backup ports.

Note – The Sun StorEdge 5210 NAS Appliance supports Etherchannel bonding, a subset of the 802.3ad specification. Refer to your switch documentation for Etherchannel bonding before attempting to set up port bonding.

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

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 system. Two or more available ports are bonded so that if the primary port fails, a secondary port in the high-availability bond automatically takes over the burden to enable services to continue without any interruptions.

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 a high-availability bond. The only requirement is that the switches must be connected to the same subnet.

Bonding Ports

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 the Network Ports" on page 12 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

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

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

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

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

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

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

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

To add alias IP addresses to the port bond, see "To Configure Network Adapters" on page 13.

Active Directory Service and Authentication

This chapter describes Active Directory Service (ADS) in detail, Lightweight Data Access Protocol (LDAP) setup, and how to change name service lookup order. For setup instructions for other name services, refer to "Name Services" on page 15.

The following topics are included in this chapter:

- "Supported Name Services" on page 61
- "Active Directory Service" on page 62
- "Setting Up LDAP" on page 67
- "Changing Name Service Lookup Order" on page 67

Supported Name Services

The system supports the following name services for both Windows networks and UNIX networks:

- ADS – Active Directory Service (ADS) is a Windows 2000 name service integrated with the Domain Name Service (DNS, see "Setting Up DNS" on page 17). ADS runs only on domain controllers. In addition to storing and making data available, ADS protects network objects from unauthorized access and replicates objects across a network so that data is not lost if one domain controller fails. When you enable and set up ADS, the system automatically performs ADS updates. See "Active Directory Service" on page 62 for more information.
- LDAP – Lightweight Data Access Protocol (LDAP) is a UNIX service that enables authentication.

- WINS – A Windows Internet Naming Service (WINS) is a service that 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 function for Windows environments similar to the function a DNS server serves for UNIX environments. See "Setting Up WINS" on page 17 for more information.
- DNS – Domain Name Service (DNS) is a service that resolves domain names to IP addresses for the system. This service enables you to identify a server by either its IP address or its name. See "Setting Up DNS" on page 17 for more information.
- NIS – Network Information Service (NIS) is a service that configures the system to import the NIS database. It administers access to resources based on the users group and host information. See "Setting Up NIS" on page 19 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 20 for more information.

Active Directory Service

For the system 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 for the Dynamic DNS capability) is recommended but not required for ADS.

After setting up ADS, you can set ADS to publish specific shares in the ADS directory. To do so, create or update Server Message Block (SMB) shares and specify the share container for each share you want to publish.

Setting up ADS involves the following:

1. Enabling ADS
2. Verifying the Name Service lookup order
3. Verifying that DNS is enabled and configured to support ADS
4. Publishing shares in ADS

▼ To Enable ADS

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

Note – Resetting the date and time will change the system clock used for most time-related operations. It will not change the secure clock used by the license management software and the Compliance Archiving Software.

4. In the navigation panel, select **Windows Configuration > Configure Domains and Workgroups**.
5. Select the **Enable ADS** checkbox.
6. In **Domain**, enter the Windows 2000 domain in which ADS is running.
The system must belong to this domain.
7. In the **User Name** field, enter the user name of a Windows 2000 user with administrative rights.

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

Note – If you enter the domain administrator name here and the ADS update fails, the domain administrator password must be changed on the domain controller. This is only required for the administrator user, and the same password may be reused. For more information, refer to the Microsoft Support Services web site, Article Q248808.

8. In the **Password** field, enter the Windows 2000 administrative user's password.

9. In the **Container** field, enter the ADS path location of the Windows 2000 administrative user in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation.

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

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

ou=users,ou=accounting

Do not include the domain name in the path.

10. 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.
12. This is normally the ADS domain or the DNS domain. When you click **Apply**, this entry is converted to all uppercase letters.
13. In the **Server** field, enter the host name of the of the Kerberos KDC server.
The KDC server name is usually the host name of the main domain controller in the ADS domain. You can leave this field blank, if the system can locate the KDC server through DNS.
14. Click **Apply** to save and invoke your changes.

▼ To Verify Name Service Lookup Order

1. Select **UNIX Configuration > Configure Name Services**.
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 **Up** and **Down** buttons to change the order in which the selected services are scanned.
3. Click **Apply** to save any changes.

▼ To Verify DNS Configuration

1. In the navigation panel, select **Network Configuration > Configure TCP/IP > Set Up DNS**.
2. If DNS is not enabled, select the **Enable DNS** checkbox.
3. If you have not entered a domain name, enter the **DNS domain name**.
This name must be the same as the ADS domain.
4. In the **Server** field, enter the IP address of the DNS server you want the system to use, and then click the **Add** button to place the server address in the **DNS Server List**.
You may add up to two servers to the list.
5. Select the **Enable Dynamic DNS** checkbox.
If you do not enable Dynamic DNS, you must add the host name and IP address manually.
6. In the **DynDNS User Name** field, enter the user name of a Windows 2000 user with the administrative rights to perform secure dynamic DNS updates.
You can leave this field blank for nonsecure updates if they are allowed by the DNS server.
7. In the **DynDNS Password** field, enter the password of the Dynamic DNS user.
8. Click **Apply** to save your changes.
If Dynamic DNS is enabled, the system immediately updates DNS with its host name and IP address.

▼ To Publish Shares in ADS

1. In the navigation panel, select **Windows Configuration > Configure Shares**.
2. Click **Add**.
3. Enter a share name.
4. (Optional) Add a comment to describe the share.
You can enter up to 60 alphanumeric characters.
5. Select a volume to share from the pull-down box.
6. (Optional) In the **Directory** field, enter an existing directory on the selected volume that you want to share.

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

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

The Container field identifies the ADS container. Enter the ADS location for the share in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation. See step 9. on page 64 for more information.

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

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

▼ To Update ADS Share Containers

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

The system updates the share container.

▼ To Remove Shares From ADS

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

Setting Up LDAP

For you to use LDAP, the LDAP server must be running.

▼ To Enable LDAP Service

1. In the navigation panel, select **UNIX Configuration > Set Up NSSLDA**P.
2. To enable LDAP, check the **Enable NSSLDA**P checkbox.
3. In the **Domain** field, enter the domain name of the LDAP server; for example, `foo.com`.
4. In the **Password** field, enter the password set on the LDAP server.
5. In the **Server** field, enter the IP address of the LDAP server.
6. In the **Proxy** field, enter the proxy domain, depending on the server settings.
7. Click **Apply** to save the settings.

Changing Name Service Lookup Order

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

▼ To Set the Order for User, Group, Netgroup, and Host Lookup

1. In the navigation panel, select **UNIX Configuration > Configuring Name Services**.
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 the Up or Down buttons to move it up or down.

The service at the top of the list is used first in user lookup.

- 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.

To configure Windows security, refer to "Configuring Windows Security" on page 15.

This chapter includes the following:

- "Local Groups" on page 69
- "Configuring Privileges for Local Groups" on page 70
- "Configuring Hosts" on page 73
- "Mapping User and Group Credentials" on page 75
- "Setting File Directory Security" on page 82

Local Groups

The requirements for Sun StorEdge 5210 NAS Appliance built-in local groups are different from those of a Windows system. For 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 Common Internet File System (CIFS) networking.

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

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

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

Configuring Privileges for Local Groups

Privileges provide a secure mechanism for assigning 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 5210 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 back up and restore files to which they would normally not have access.

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

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

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

TABLE 7-1 Supported Privileges

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

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

TABLE 7-2 Default Group Privileges

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

Ownership Assignment

By default, the Domain Admins group of the domain that the Sun StorEdge 5210 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 5210 NAS Appliance, however, the domain administrator is always assigned membership in the local administrators group. However, the domain administrator is not listed as a member of this group, so you cannot revoke its membership. Because there are no local users, and thus no local Windows administrators, the domain administrator group must have administrative control on the Sun StorEdge 5210 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 local groups.

▼ To Add or Remove a Member of a Group

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

▼ To Configure NT Privileges

1. In the navigation panel, select Windows Configuration > Configure Groups.
2. In the Groups box, select the group for which you want to assign privileges.

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 file system and have read and write access to all files and directories in that file system.

A root user on an NFS client has root privileges on the Sun StorEdge 5210 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

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

3. Enter the host name.

This is the name by which the host is known on the system. The host name can include alphanumeric (a-z, A-Z, 0-9), "-" (dash) and "." (period) characters only. The first character must be alphabetical (a-z or A-Z only).

4. 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 5210 NAS Appliance.

6. Click Apply to save your changes.

▼ To Edit Host Information

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

2. Select the host for which you want to edit information and click Edit.

3. Revise the 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.

▼ To Remove a Host Mapping for a Particular Host

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

2. Select the host that you want to remove by clicking on the entry in the host list.

3. Click Remove.

4. Click Apply.

Mapping User and Group Credentials

Sun StorEdge 5210 NAS Appliance servers are designed to reside in a multiprotocol environment and provide an integrated model for sharing data between Windows and UNIX systems. Although files may be accessed simultaneously from both Windows and UNIX systems, there is no industry-standard mechanism to define a user in both Windows and UNIX environments. Objects can be created using either environment, but the access control semantics in each environment are vastly different. This section addresses credential mapping. For details about the interaction between user or group credential mapping and the securable objects within the system, refer to "Mapping and Securable Objects" on page 179.

Credential mapping is used to establish an equivalence relationship between a UNIX user or group defined in a local configuration file or Network Information Service (NIS) database with a Windows domain user or group defined in a Windows Security Account Manager (SAM) database. User and group mapping is a mechanism to establish credential equivalence on the Sun StorEdge 5210 NAS Appliance to provide common access using either environment.

UNIX Users and Groups

UNIX users and groups are defined in local configuration files (`passwd` and `group`) or in a NIS database. Each user and group is identified using a 32-bit identifier known, respectively, as a user identifier (UID) or a group identifier (GID). Most UNIX systems use 16-bit identifiers but this has been extended to 32 bits on the Sun StorEdge 5210 NAS Appliance to avoid limitations imposed by the range of a 16-bit number. Although the UID or GID uniquely identifies a user or group within a single UNIX domain, there is no mechanism to provide uniqueness across domains. Traditionally, the value zero is applied to the root user or group. Root is granted almost unlimited access for administration tasks.

Windows Users and Groups

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

The format of a SID is as follows:

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

The fields within the SID structure are described in TABLE 7-3.

TABLE 7-3 Fields in the SID

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

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

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

To integrate with the Windows domain model, each Sun StorEdge 5210 NAS Appliance also generates a SID to define its local domain. The SID is generated using an algorithm that produces four subauthorities. The first subauthority has the value 4, which represents a nonunique authority. The other three subauthorities are

generated using an algorithm that includes the current time and one of the system's MAC3 addresses to ensure uniqueness. This SID is used to represent both local and NIS users by having the UNIX UID or GID appended to it. This SID is stored in the equivalent of a local SAM database.

Credential Mapping

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

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

The mapping format is as follows:

UNIX-username : UID : Windows-username : NTDOMAIN : RID

UNIX-groupname : GID : Windows-groupname : NTDOMAIN : RID

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

username : password : UID : GID : comment : home-directory : shell

groupname : password : GID : comma-separated-list-of-usernames

User Mapping

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

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

User Mapping Policy Settings

There are four user mapping policy settings.

- `MAP_NONE` specifies that there is no predefined mapping between Windows users and UNIX users. A new unique UNIX UID will be assigned to the Windows user. The UID is tested for uniqueness by a search through the currently configured `passwd` database and the user map file and selection of a new UID. Typically the new UID will be one larger than the largest value found in the search. The `passwd` database may comprise the local NAS `passwd` file and the NIS `passwd` file, if NIS is enabled. In this case, the mapping entry must be modified by hand if the Windows user should be mapped to an existing UNIX user.
- `MAP_ID` specifies that the UNIX UID is the Windows user's RID. No lookup is done on the `passwd` database.
- `MAP_USERNAME` specifies that the Windows user's user name is looked up in the `passwd` database. If a match is found between the Windows user name and the UNIX user name, the UNIX UID is taken from the matching entry. If no match is found, a unique UNIX UID is generated using the mechanism specified in `MAP_NONE` mechanism.
- `MAP_FULLNAME` specifies that the Windows user's Windows full name is looked up in the `passwd` database. A match is attempted with the UNIX comment field of each password entry. Only the full name entry of the comment field in the `passwd` database is compared with the Windows full name. If a match is found, the UNIX UID from the matching entry is used. If no match is found, a unique UNIX UID is generated as in the `MAP_NONE` mechanism.

The appropriate group credentials for the Windows user are obtained using the group mapping algorithm. For details, refer to "Group Mapping" on page 78.

User Mapping Policy Example

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

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

Group Mapping

Group mapping is used to create an equivalence relationship between a UNIX group and a Windows group. To determine the appropriate UNIX GID for a Windows user, the group map is searched using the user's Windows domain name and Windows primary group name. If a match is found, the map entry defines the UNIX GID to

which the Windows user's group will be mapped. If there is no matching entry in the group map, the UNIX GID is determined by the group map policy setting, and a new entry is created in the group map, with the exception of the `MAP_UNIXGID` policy.

Group Mapping Policy Settings

There are four group mapping policy settings:

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

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

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

Group Mapping Policy Example

The following example shows a group map that makes the `HOME\BASE\Domain Admins` group equivalent to the UNIX `wheel` group and the `HOME\BASE\Domain Users` group equivalent to the UNIX `users` group.

```
wheel:800:Domain Admins:HOME\BASE:1005
users:100:Domain Users:HOME\BASE:513
```

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

```
map.users=MAP_NONE
```

```
map.groups=MAP_NONE
```

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

```
map.users=MAP_USERNAME
```

```
map.groups=MAP_ID
```

Built-In Credential Mapping

The UNIX root identifier, 0 (UID or GID), is always mapped to the local Administrators group. The SID for the local Administrators group is a built-in (predefined) Windows SID `S-1-5-32-544`. This mapping conforms to the ownership assigned by Windows to files created by the Domain Administrator. Ownership of such files is always assigned to the built-in local Administrators group to provide domain independence; that is, to avoid losing access to these files in the event that the system is moved from one Windows domain to another. In the Windows permissions display box, this SID appears as `hostname\Administrators`, where `HOSTNAME` is the Sun StorEdge 5210 NAS Appliance host name.

▼ To Define the Mapping Policy

- 1. In the navigation panel, select Windows Configuration > Manage SMB/CIFS Mapping > Configure Mapping Policy.**
- 2. Select one of the following user mapping settings from the Windows <--> UNIX User Mapping Choice section.**
 - **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 5210 NAS Appliance from both environments.
 - **Map by Full Name** – Select this option to map UNIX and Windows users who have identical full names.
- 3. Select one of the following group mapping settings from the Windows <--> UNIX Group Mapping Choice section.**
 - **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.

For more detail about the interaction between user or group credential mapping and the securable objects within the system, refer to "Mapping and Securable Objects" on page 179.

▼ To Map Windows Groups and Users to UNIX Groups and Users

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

2. Click Add.

3. In the NT User box, enter the following information:

- Account – The NT account name of the user or group you want to map.
- RID – The relative identifier that uniquely identifies the NT user or group within the NT domain.

4. In the UNIX User box, enter the following information:

- Name – The UNIX user or group name to which you want to map the specified NT user or group.
- ID – The identifier that uniquely identifies the UNIX user or group within the UNIX domain.

5. Click Apply to save your changes.

For more detail about the interaction between user or group credential mapping and the securable objects within the system, refer to "Mapping and Securable Objects" on page 179.

Setting File Directory Security

There are two methods for setting file directory security:

- "Setting File Directory Security in Workgroup Mode" on page 82
- "Setting File Directory Security in Domain Mode" on page 82

Setting File Directory Security in Workgroup Mode

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

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

See "To Add a New SMB Share" on page 87 for instructions on setting share-level security while adding a share. See "To Edit an Existing SMB Share" on page 89 for instructions on setting share-level security while editing shares.

Setting File Directory Security in Domain Mode

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

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

Note – The Sun StorEdge 5210 NAS Appliance supports security on files and directories only. 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.**
3. **In the Map Network Drive dialog box, select a drive letter from the Drive pull-down menu box.**
4. **Locate and select the Sun StorEdge 5210 NAS Appliance.**
5. **Click OK.**
6. **From the Windows Explorer window, right-click on the system share for which you want to define user-level permissions.**
7. **Select Properties from the pull-down menu.**
8. **Select the Security tab in the Properties dialog box.**
9. **Click the Permissions button.**
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 5210 NAS Appliance.

The following topics are included:

- "Shares" on page 85
- "Managing Quotas" on page 92
- "Setting Up NFS Exports" on page 97

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 5210 NAS Appliance.

A shared resource, or share, is a local resource on a server that is accessible to Windows clients on the network. On a Sun StorEdge 5210 NAS Appliance, it is typically a file system volume or a directory tree within a volume. Each share is identified by a name on the network. To clients on the network, the share appears as a complete volume on the server, and they do not see the local directory path directly above the root of the share.

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

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

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

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

Static Shares

A static share is created to allow a 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 shown in TABLE 8-1.

TABLE 8-1 Share Path Examples

Share Name	Directory Path
<code>bob</code>	<code>/vol1/home/bob</code>
<code>sally</code>	<code>/vol1/home/sally</code>

If it is inconvenient to define and maintain a static home directory share for each Windows user who has access to the system, you can use the autohome feature. See "Autohome Shares" on page 91 for more information.

Configuring Static Shares

You use the Configure Shares panel 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. 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.

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 34.

▼ To Add a New SMB Share

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

2. Click **Add**.

3. **Type the name of the share you want to add in the Share Name field.**

This is the name that users see on the network. The name cannot be longer than 15 characters. The following characters are invalid:

= | : ; \ " ' ? < > * /

4. **(Optional) 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 system 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 5210 NAS Appliance.

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

7. **Enter an existing directory in the Directory field.**

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

Note – Do not leave the Directory field blank.

8. **(Optional) In the Container field, specify the ADS container in which you want 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.

9. **To specify the container, enter the ADS path location for the share in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation.**

See "To Publish Shares in ADS" on page 65 for more information.

10. Enter the user ID (UID), group ID (GID), and password, if available.

The User ID, Group ID, and Password fields are only available if you enable Windows Workgroup mode (not NT Domain mode). Refer to "Configuring Windows Security" on page 15 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 5210 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 system assumes that the client performs no authentication and explicitly asks for permission through the use of a password with every share-connection request.

You can create multiple shares for the same directory with different UIDs, GIDs, and passwords. You can then give each user a password for a specific share. You can also manage individual user and group limitations on the amount of file volume space or number of files used through quotas. For more information about quotas, refer to "Managing Quotas" on page 92.



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

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

11. In the Umask field, enter the file creation mask, if any, that 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 be turned off when a file is created.

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

TABLE 8-2 shows umask-to-permission examples, including the effect of the DOS read-only attribute.

TABLE 8-2 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--)

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

▼ To Edit 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**.
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. (Optional) Change the description of the share in the **Comment** field.

You can enter up to 60 alphanumeric characters.

6. Select the **Desktop DB Calls** checkbox in the **Mac Extensions** section to let the system access and set Macintosh desktop database information.

This speeds up Macintosh client file access and allows non-Macintosh clients to access Macintosh files on the Sun StorEdge 5210 NAS Appliance.

7. Change the share path by entering 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 in the **Set Up ADS** panel. Enter the ADS path location for the share in LDAP DN notation. See "To Enable ADS" on page 63 for more information.

9. Enter the user ID, group ID, and password, if available.
See step 10. on page 88 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 11. on page 88.
11. Click Apply to save your changes.

▼ 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 5210 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 ways described in the following subsections.

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 5210 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 5210 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 5210 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 5210 NAS Appliance icon in the **My Network Places** window.

If they map the network drive, they need the UNC path for the Sun StorEdge 5210 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 5210 NAS Appliance on the network.

If ADS is installed, users can connect by clicking on a Sun StorEdge 5210 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 5210 NAS Appliance which consists of a computer name and share name as follows: `\\computer_name\share_name`.

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 15 minutes of inactivity, which results in removal of the autohome share from the list of published shares. This is normal CIFS protocol behavior. If the user clicks the server name or otherwise attempts to access the system (for example, in an Explorer window), the share automatically reappears.

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

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

▼ To Enable Autohome Shares

1. In the navigation panel, select **Windows Configuration > Configure Autohome**.
2. Select the **Enable Autohome** checkbox.
3. Enter the **autohome path**.
For more information on the path, see "Autohome Shares" on page 91.
4. Enter the **ADS container**.
For more information, see "Active Directory Service" on page 62.
5. Click **Apply** to save your changes.

Managing Quotas

The Manage Quotas panels let you administer quotas on Sun StorEdge 5210 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 how many files can be written to it.

See "Configuring User and Group Quotas" on page 92 to set space and file limits for users and groups. Refer to "Configuring Directory Tree Quotas" on page 95 to set space and file limits for specific 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 settings for the default user and default group are the settings used for all users and groups that do not have individual quotas.

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 terabytes. For the number of files, the hard limit can be no more than 4 billion files.

The root user and root group are automatically set to have no hard or soft limits for space or files and cannot have quotas defined.

▼ 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** pull-down menu.
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**.
2. Click **Users** if you are configuring a user quota, or **Groups** if you are configuring a group quota.
3. From the drop-down **Volume** list, select the name of the file volume for which you are adding a quota.

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

4. To add a quota for a user or group, click **Add**.
5. Select whether the designated user or group belongs to a **UNIX** or **NT** environment by clicking on the appropriate option button.
6. Select the appropriate user or group name (and domain name for NT users or groups).
7. Set the disk space limits for the selected user or group.

Choose among 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 allow unlimited space to the user or group.
- **Custom** – Choose this option to set a particular limit. Select whether the quota is displayed in kilobyte, megabyte, or gigabyte. 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 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.

9. Click Apply to save your changes.

▼ **To Edit a User or Group Quota**

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

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

3. From the drop-down Volume list, select the name of the file volume for which you are editing quotas.

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

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

5. Edit the disk space limits for the selected user or group.

Choose among 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 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 kilobyte, megabyte, or gigabyte. 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 among 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.

▼ To Delete a Quota

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

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** panel lets you administer quotas for specific directories in the file system. Directory tree quotas (DTQs) 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.

▼ To Create a Directory Tree With a DTQ

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

6. Specify the full path of the directory in the Path field.

Underneath the Path field is a box that shows the directory tree structure for the file volume you selected. To view the contents of a folder, click the symbol next to the folder, or double-click the folder icon. Then select the directory that will contain the new directory that you are creating. Continue until the full path of the directory is shown in the Path field.

7. Select the disk space limit for the directory in the Disk Space Limits section, selecting either No Limit or Custom.

- Select No Limit to allow unlimited disk space for the directory.
- Select Custom to define the maximum disk space that the directory can occupy.

8. Choose whether the quota is reported in megabyte or gigabyte, and enter the disk space limit in the Max Value field.

Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.

9. In the File Limits field, select the maximum number of files that can be written to this directory, either No Limit or Custom.

- Select No Limit to allow an unlimited number of files to be written to this directory.
- Select Custom to assign a maximum number of files. Then enter the file limit in the Max Value field.

10. Click Apply to add the quota.

▼ **To Edit an Existing Directory Tree Quota**

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

2. Select the quota you want to edit from the table, then click Edit.

3. Edit the name that identifies this directory tree quota in the DTQ Name field.

Path is a read-only field that shows the path of the directory.

4. In the Disk Space Limits section, select the disk space limit for the directory, selecting either No Limit or Custom.

- Select No Limit to allow unlimited disk space usage for the directory.
- Select Custom to assign a maximum amount of disk space.

5. Choose whether the quota is reported in megabyte or gigabyte, and enter the disk space limit in the Max Value field.

Entering a Custom value of 0 (zero) is equivalent to choosing No Limit.

6. In the File Limits section, select the maximum number of files to be written to this directory, selecting either No Limit or Custom.

- Select No Limit to enable you to write an unlimited number of files to this directory.
 - Select Custom to assign a maximum number of files.
7. Enter the file limit in the Max Value field.
 8. Click Apply to save your changes.

Note – When you move or rename a directory that contains a DTQ setting, the system automatically updates the DTQ's path specification.

▼ 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 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 73 for information about trusted hosts.

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

▼ To Create Exports

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

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

2. **Click the Add button to add an export.**
3. **In the Volume box, select the volume for which you want to grant UNIX NFS host access.**
4. **In the Path box, specify the directory for which you want to grant UNIX NFS host access.**

Leaving this field blank exports the root directory of the volume.

5. **In the Access section, specify whether the hosts have Read/Write, Read/Only, or No Access privileges on the selected volume.**

6. **In the Hosts section, select the host or hosts for which you are defining an NFS export.**

Choose from the following:

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

7. **In the Map Root User section, select a method for mapping the user ID for root users.**

Choose from the following:

- **Anonymous users** – To map the user ID of root users to the user ID of anonymous users, select this option button.
- **Root User** – To map the user ID of root users to the user ID of root (UID=0), select this option button.
- **Map to UID** – To assign a specific user ID, select this option and enter the user ID.

8. **Click Apply to save the export.**

9. In the Configure Exports panel, verify that the correct path, host, and access rights are shown for the export you created.

▼ To Edit Exports

1. In the navigation panel, select UNIX Configuration > Configure NFS > Configure Exports.
2. Select the export you want to change, and click the Edit button.
3. To change the Access rights, click Read/Write, Read/Only, or No Access.
The Hosts section is read-only.
4. Click Apply to save your changes.
5. In the Configure Exports panel, verify that the correct path, host, and access rights are shown for the export you edited.

▼ To Remove Exports

- Click on the export in the Configure Exports panel, and click the Trash button.

System Options

This chapter provides instructions for activating options you can purchase for the Sun StorEdge 5210 NAS Appliance. Additionally, it provides details about the following options:

- Sun StorEdge File Replicator, which allows you to duplicate data from one volume onto a mirrored volume on a different Sun StorEdge 5210 NAS Appliance (typically used for transaction-oriented systems)
- Compliance Archiving Software, which allows you to enable volumes to follow compliance archiving guidelines for data retention and protection

This chapter includes the following topics:

- "Activating System Options" on page 101
 - "Sun StorEdge File Replicator" on page 102
 - "Compliance Archiving Software" on page 113
-

Activating System Options

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

▼ To Activate an Option

1. In the navigation panel, select **System Operations > Activate Options**.
2. Click **Add** to add the license.
3. In the **Add License** dialog box enter the module name provided by Sun (for example, **Sun StorEdge File Replicator**).

4. 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.

5. Enter the expiration date provided by Sun in the format YYYYMMDD.

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

Note – When a compliance license expires or is removed, the system will maintain compliance rules, but no new compliance volumes can be created. Refer to “Compliance Archiving Software” on page 113 for more information about the Compliance Archiving Software.

6. Enter the license key provided by Sun.

7. Click Apply to activate the option.

For Sun StorEdge File Replicator, you must perform additional steps on the mirrored server. Refer to “To Activate Sun StorEdge File Replicator on the Remote Server” on page 105 for instructions.

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

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

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

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

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

Sun StorEdge File Replicator

Sun StorEdge File Replicator software enables you to maintain exact duplicates of data on two servers.

Sun StorEdge 5210 NAS Appliance Mirroring

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

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

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

When setting up your systems, designate the roles of the ports connecting the mirroring servers to one another (see "To Configure the Dedicated Network Ports" on page 104). Then configure mirroring on the active and mirror systems using the Web Administrator interface (see "Configuring Mirrored File Volumes" on page 104). Configure each system independently.

Preparing for Mirroring

Before you begin, make sure you meet the following requirements:

- 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 100 megabit Ethernet or 1000 megabit Ethernet. The servers may be connected through a switch or router. If you are connecting the servers to a router, be sure to configure the static route setting to ensure that the mirroring data is directed through the private route. If you are connecting the servers to a switch, create a virtual LAN (VLAN) for each server to isolate network traffic.
- Both servers must have the same version of the operating system installed.
- The active file volumes to be mirrored must be at least 1 gigabyte.

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

▼ To Configure the Dedicated Network Ports

1. In the navigation panel of the active server, select **Network Configuration > Configure TCP/IP > Configure Network Adapters**.
2. If you have not done so already, assign the 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 12.

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, 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 164.
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 gigabyte can be mirrored. Once a file volume is mirrored, the original file volume cannot be renamed while the mirroring connection is maintained.

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

Mirror Buffer

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

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

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

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

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

▼ To Activate Sun StorEdge File Replicator on the Remote Server

After you have activated the Sun StorEdge File Replicator option (see "Activating System Options" on page 101), 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 volumes 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.**

▼ To Add a File Volume

1. **On the navigation panel, select File Replicator > Manage Mirrors.**
2. **Click Add.**
3. **From the Volume pull-down menu, select the file volume to be mirrored.**
The file volume to be mirrored must be equal to or larger than 1 gigabyte.
4. **Enter a distinct name for the mirror server in the Mirror Host field.**
5. **Enter the IP address of the mirror system.**
This should be the IP address chosen for the mirroring NIC on the mirror system.
6. **(Optional) Enter the Alternate IP Address.**
In the event that the first IP address becomes unavailable, the server uses the alternate IP address to maintain the mirror.
7. **If an administrative password is required to access the mirror server, enter it in the Password field.**
If there is no administrative password, leave this field blank. Always protect your servers with passwords.
8. **Enter the size (in megabytes) of the mirror buffer.**
The file volume free space on the active server is reduced by the allocation size of the mirror buffer.
9. **Make sure there is no I/O activity to the source file volume on the active server while the mirror is being created, and then click Apply to create the mirror.**
The mirror creation process begins. When the mirror reaches an In Sync status in the Manage Mirrors panel, the mirrored file volume is mounted as read-only. I/O activity can resume once the mirror reaches In Sync status.

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

▼ To Edit a Mirror

1. **In the navigation panel, select File Replicator > Manage Mirrors.**
2. **Select the mirror that you want to edit from the table.**
3. **Click Edit.**
The file volume name and mirror host are read-only fields.
4. **Edit the 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.**

▼ To Correct a Cracked Mirror

In the event a mirror cracks (this happens if the connection between the two servers is unavailable for some time or if the mirror buffer is too small and there are many writes to the master volume), do the following:

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

This file system can be used for backup or any read-only activity.

You can also combine checkpoints with the Mirroring functionality. When a checkpoint is created on the active server, the checkpoint also gets mirrored to the mirrored server. This can be used for scheduled backups or to give read-only checkpoint access to other users and applications.

Setting Warning Thresholds

In the File Replicator > Set Threshold Alert panel you can set the threshold alert for all mirrored file volumes. The threshold alert is the percentage of mirror buffer use at which a warning is sent to designated recipients.

The mirror buffer stores file system write transactions while they are being transferred to the mirror server. Increases in write activity to the active server or a damaged network link can cause the transference of write transactions to the mirror server to “back up” in the mirror buffer. If the mirror buffer overruns because of this process, the mirror is cracked and no further transactions occur between the active server and the mirror server until the mirror is reestablished. Once full communication is restored, the system automatically begins the mirror resync process until the mirrored file volume is back in sync.

To prevent this situation, the system automatically sends warnings through email notification, the system log file, Simple Network Management Protocol (SNMP) traps, and the LCD panel when the mirror buffer is filled to certain threshold percentages.

▼ To Set Up the Threshold Alert

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

2. Select the Mirroring Buffer Threshold 1.

This is the percentage of mirror buffer usage that triggers the first alert. The default value is 70 percent. This means that when the mirror buffer is 70 percent full, an alert is automatically issued.

3. Select the Mirroring Buffer Threshold 2.

This is the percentage of mirror buffer usage that triggers the second alert. The default value is 80 percent.

4. Select the Mirroring Buffer Threshold 3.

This is the percentage of mirror buffer usage that triggers the third alert. The default value is 90 percent.

5. Select the Alert Reset Interval (Hours).

This is the amount of time the system waits before reissuing an alert if the condition recurs within the interval.

For example, if you set the Mirroring Buffer Threshold 1 to be 10 percent and the Alert Reset Interval to two hours, the first alert is issued when the mirror buffer is 10 percent full. The system will not issue the Threshold 1 alert again for the next two hours. If at that time the mirror buffer usage is still beyond the 10 percent threshold (but not beyond Thresholds 2 or 3), the Threshold 1 alert is issued again.

The default value for this field is 24 hours.

6. Click Apply to save your changes.

Breaking the Connection Between Mirror Servers

To promote a file volume on the mirror server (for example, if 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 unavailable 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**.
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 109.

Promoting a Mirrored File Volume

In the event that the active server fails, the mirror server provides high availability for mirrored file volumes. To make a mirrored file volume available to network users, you must promote the file volume. You must first break the mirror connection, then promote the mirrored file volume and configure its access rights. Once a mirror connection is broken and the mirrored file volume promoted, the original and mirrored file volumes are completely independent.



Caution – The mirror of a strict compliance-enabled volume cannot be promoted.

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

To promote a file volume on the mirror server, you must first break the mirror connection. See "Breaking the Connection Between Mirror Servers" on page 108 for instructions.

▼ To Promote a File Volume on the Mirror Server

1. In the navigation panel of the mirror server, select **File Replicator > Manage Mirrors**.
2. Click **Promote**.
3. 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. Server Message Block (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 97.

Reestablishing a Mirror Connection

This procedure describes how to reestablish a mirror connection after the active server fails and you promote the file volume on the mirror server. The promoted file volume is now the most up-to-date version and functions completely independently of the out-of-date file volume on the active system. To recreate the mirror connection, you must mirror the up-to-date file volume back to the active server, and then mirror the file volume back to the mirror server as you did originally.

Note – If the mirrored file volume was not promoted, do not follow these instructions. The active system automatically brings the mirror back to an In Sync state when it is back online.

In the examples that follow, *Server 1* is the active server, and *Server 2* is the mirror server.

▼ To Reestablish a Mirror Connection

1. Make sure the mirror on Server 1 is broken.

See "To Break the Mirror Connection on the Active Server" on page 111.

2. Delete the out-of-date file volume on Server 1.

See "To Delete the Out-of-Date File Volume From Server 1" on page 111.

3. Mirror the up-to-date file volume from Server 2 back to Server 1.

See "To Mirror the Up-to-Date Volume From Server 2 to Server 1" on page 111.

4. Change the role on Server 2.

See "Changing Volume Roles" on page 112.

Server 1 is now active again, and Server 2 is the mirroring target.

▼ To Break the Mirror Connection on the Active Server

1. Open a Web browser window to Server 1.
2. In the navigation panel, select File Replicator > Manage Mirrors.
3. Select the mirror connection you want to break.
4. Click Break.

▼ To Delete the Out-of-Date File Volume From Server 1

1. In the navigation panel of Server 1, select File Volume Operations > Delete File Volumes.
2. Select the file volume that was being mirrored.

Because the file volume on the mirror server has been promoted and is now the current version, the file volume on the active server is out of date and must be deleted.



Caution – Before completing the following step, be sure you are deleting the out-of-date source file volume on the active server. Also, be sure that the up-to-date file volume on the mirror server is verified and promoted first.

3. Click Apply to delete the out-of-date file volume.

▼ To Mirror the Up-to-Date Volume From Server 2 to Server 1

1. Open a Web browser window to Server 2.
2. In the navigation panel, select File Replicator > Manage Mirrors.
3. Click Add.
4. Select the file volume to be mirrored from the Volume pull-down menu.
5. 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 "Sun StorEdge 5210 NAS Appliance Mirroring" on page 103.

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 112 for more information.

You have reestablished the original mirroring connection.

Changing Volume Roles

An administrator can switch roles between an active volume and the mirror volume. Changing volume roles enables the active volume to function as the mirror volume and vice versa; however, the original configuration on each volume remains unchanged. Changing roles is not a disaster recovery function.

Note – The volumes must be 100 percent in sync to change roles.

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

▼ To Change Roles

1. In the navigation panel, click **File Replicator > Manage Mirrors**.
2. Select a volume in the **Volume** column.
3. Click **Change Roles**.
4. Click **Yes** to confirm.

Compliance Archiving Software

The Sun StorEdge 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 record 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 in consultation with information-management compliance and enterprise content management industry experts to help address the most stringent requirements for electronic storage media retention and protection. Compliance Archiving Software uses WORM (write once, read many) files in accordance with compliance rules.

Enabling Compliance Archiving

The Compliance Archiving Software is available in both a stringent form (referred to as “mandatory enforcement”) and a less stringent form (referred to as “advisory enforcement”).

If the Compliance Archiving Software is activated (see “Activating System Options” on page 101), you can choose to enable compliance with advisory or mandatory enforcement when you create a volume.

Note – Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorEdge 5210 NAS Appliance hardware. In particular, the Sun StorEdge redundant array of independent disks (RAID) controller arrays should not be connected to any device or network other than a private Fibre Channel connection to the network attached storage (NAS) head and any expansion units.

Note – To ensure the strongest possible enforcement of your data retention policies, you should also provide for the physical security of your Sun StorEdge 5210 NAS Appliance. Software-controlled data retention can be no stronger than the physical safeguards used to control access to the system’s hardware.



Caution – You should not enable compliance archiving on volumes that will be used by applications and users that are not aware of the 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 “To Create a File Volume or Segment Using the Create File Volume Panel” on page 35 to create a compliance-enabled volume.

Compliance With Mandatory Enforcement

Compliance with mandatory enforcement means adhering to directives about data protection, retention, and privacy, including the following:

- You cannot destroy a compliance volume with mandatory enforcement.
- You cannot destroy a WORM file until the retention period has been met.
- You can increase or decrease the retention period of a volume, but you can only increase the retention period of a WORM file.
- You cannot restore a WORM file from a checkpoint.



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

Compliance With Advisory Enforcement

In contrast to compliance with mandatory enforcement, compliance with advisory enforcement includes the following:

- An authorized administrator can destroy compliance WORM files and compliance volumes (using the audited delete feature).

Note – Before a volume is deleted, the audit logs within that volume must be retained by being copied to a different file system. Otherwise, those logs will be lost.

- An authorized administrator can increase and decrease retention time.
- An authorized administrator can restore WORM files from a checkpoint (using the audited delete feature).
- The root user can change the default retention time (zero days).

Note – Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See “Managing Trusted Hosts” on page 181.

When a compliance-enabled volume with advisory enforcement is upgraded to mandatory enforcement, the default retention period for that volume becomes permanent. This can be changed on the Edit Properties panel.

Note – Upgrading a compliance-enabled volume with advisory enforcement is not supported for gateway configurations.

Compliance Auditing

Compliance auditing provides a text-based log of attempted efforts to modify or delete data and is enabled through the use of the Data Retention Audit Service (DRAS) API, which includes the following features:

- Accountability of changes and attempted changes to retained files
- A logging mechanism through which auditable events are stored
- Protection and preservation of the audit log for the life of the system
- Audit log information in a readily viewable format, and secure access to the audit log through standard system access protocols

Auditable events are as follows:

- Retention of a file
- Extension of the retention period on a retained file
- Requests to unlink (delete) a retained file
- Requests to write to a retained file
- Requests to rename a retained file
- Requests to remove a directory
- Requests to rename a directory

File Size Limitations

Compliance volumes reserve an amount of free space to guarantee that auditable operations on the volume can be logged. When the free space remaining on a compliance volume falls below this limit, auditable operations are not executed. A

message is logged indicating that there is not enough space to execute both the operation and the audit, and a warning email is sent, if email has been configured on the system.

Audit Log

The audit log for each compliance-enabled volume resides in that volume's root directory.

Audit log records are text-based and can be accessed through network protocols, including NFS and CIFS. The `.audit$` directory must be included in the share path for the contents to be viewed by clients running Windows 2000 or XP. Refer to "Shares" on page 85 for details about creating shares.

The audit log format is shown in TABLE 9-1.

TABLE 9-1 Audit Log Format

Field	Length	Description
Version	7	The Data Retention Audit Service version number
Serial Number	11	A unique sequence number
Length	5	The length of the audit record
Timestamp	21	The date and time at which the event occurred
TID	11	The thread ID of the thread from which the event was executed
Volume ID	11	The volume ID of the volume on which the audit was performed
Protocol	9	The network protocol through which the operation was requested
Inode	11	The file system inode number of the file
Client IP Address	16	The IP address of the client from which the operation was requested
Server IP Address	16	The IP address through which the client request was received
UID	11	The user credential
GID	11	The primary group credential
Operation	8	The audit event
Status	Variable	The result of the operation

TABLE 9-1 Audit Log Format (*Continued*)

Field	Length	Description
Domain	Variable	The Windows domain that the user belongs to, if available
File/Directory Name	Variable	The name of the file or directory on which the operation was performed, if available
Path/Extra Data	Variable	Extra information from the audit, if available

Additional Compliance Archiving Features

For a technical overview of the features and programming interface for the Compliance Archiving Software, see Appendix C.

To change compliance archiving settings, see “Configuring the Compliance Archiving Software” on page 198.

Monitoring the System

This chapter describes the monitoring functions of the Sun StorEdge 5210 NAS Appliance. 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.

The following topics are included:

- "SNMP Monitoring" on page 120
- "Viewing System Status" on page 121
- "System Logging" on page 122
- "System Auditing" on page 125
- "Environmental Status" on page 127
- "Usage Information" on page 131
- "Viewing Network Routes" on page 134
- "Monitoring System Components" on page 135
- "Viewing Backup Job Status" on page 139

SNMP Monitoring

You can conduct Simple Network Management Protocol (SNMP) monitoring by enabling SNMP communications. The Sun StorEdge 5210 NAS Appliance supports SNMP monitoring only (not SNMP management).

To interpret Message Information Blocks (MIBs), you need the MIB files. The MIB files are installed with the image in the *boot_directory/www/data/mib* directory; for example, */cvol/nf1/www/data/mib*.

The MIB files are also available for download from <http://sunsolve.sun.com>. Refer to your network management application documentation for information about how to use these files.

▼ To Set Up SNMP

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

Configure SNMP

Enable SNMP

Server SNMP Community:

Contact Info:

System Location:

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"/>

2. Select the **Enable SNMP** checkbox to enable SNMP.
3. In the **Server SNMP Community** field, enter the SNMP community to which the Sun StorEdge 5210 NAS Appliance belongs.
4. In the **Contact Info** field, enter the name of the person who is responsible for this system.

5. In the System Location field, enter the network location.

This location can be physical or logical.

6. To add a new target address, provide the following information in an empty row of the SNMP table:

- Destination IP Address – Enter the TCP/IP address for the server you want to designate as an SNMP trap destination in the event of system errors.
- Port # – Enter the port to which the system is to send traps. The default value is port 162.
- Version – Choose the SNMP version (either 1 or 2) from the pull-down menu.
- Community – Enter the community string for the trap destination.
- Enable – Select the checkbox in this column to enable this target address to become a trap destination.

7. To remove a target address, select the line you want to remove and click the Trash button.

8. Click Apply to save your changes.

Viewing System Status

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 you are calling Customer Support and can provide the first indication of what has failed in some cases.

▼ To View System Status

- Click the Home button in the toolbar.

The screen provides a read-only display of the data listed in TABLE 10-1.

TABLE 10-1 System Status Display

Name	Display
Name	The server name
Model	The system model
Serial #	The unique serial number of the system
Up Time	The amount of time elapsed since the system was last turned on
CPU Load	The current and peak processor load
OS Version	The version of the operating system on the server
Web Admin Version	The version of the Web Administrator on the system
Features Enabled	Any optional features enabled on the system

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 the local disk to prevent the log from disappearing on system shutdown. When it first starts, the system creates a temporary log file in volatile memory to retain any errors that might occur during initial startup.

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

Note – Changes to drive configuration (such as removing or inserting a drive) may take up to 30 seconds to appear on the event log. As such, if there are multiple changes within that time frame, some events may not be reported.

The screenshot shows a window titled "Display System Log". At the top, there is a "Log Name:" field. Below it is a table with three columns: "Date", "Time", and "Description". The table contains 18 rows of event data, all with a date of 12/20/04 and a time of 18:48:08, except for the last two rows which are at 18:48:06. Each row's description is "nmir: nmdeseq: Write error on xid [value] length 32768". Below the table is an "Event Types" section with icons for Emergency (red X), Alert (red circle), Critical (red X), Error (red X), Warning (yellow triangle), Notice (green triangle), Information (blue circle), and Debug (green bug). Each icon has a corresponding checkbox, all of which are checked. At the bottom of the window are four buttons: "Refresh", "Print Log", "Save As...", and "Silence Alarm".

Date	Time	Description
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11242 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11242 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11240 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11238 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11238 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11236 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11234 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11232 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11230 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11228 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11226 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11222 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11222 length 32768

▼ To View the System Log









1. In the navigation panel, select **Monitoring and Notification > View System Events > Display System Log**.
2. Check all **Event Types** you want to view.
See "System Events" on page 124 for more information.
3. Click **Refresh**.

Note – If your system log contains error messages stating “Unowned SFS2” volumes, call Technical Support for assistance.

System Events

The system log logs eight types of system events. Each event is represented by an icon, shown in TABLE 10-2.

TABLE 10-2 System Event Icons

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

System Auditing

System auditing allows the system administrator to audit particular system events by storing records of those events in log files. Auditing is separate from `syslog`; the system audit trail is written to binary files on the local system.

System auditing must be enabled by the system administrator with a file volume configured as the audit trail storage volume. Auditing can be enabled and configured through the Web Administrator, the operator menus, or CLI commands.

Audit Configuration

You must specify the audit volume, which can be any non-system volume. Although the system does not force that volume to be used only for auditing, you should not use audit volumes for general purpose storage.

The maximum audit log file size has a default value, but it may be changed by the user. Once the current audit log reaches approximately this size (it may vary by about 1 kilobyte), the log file is closed, and a new log file is created.

▼ To Set Up System Auditing

1. **In the navigation panel, select Monitoring and Notification > Enable System Auditing.**
2. **To enable System Auditing, select the Enable System Auditing checkbox.**
3. **Select a volume for storing system auditing logs.**

Selectable volumes are non-system volumes. You should create special purpose audit volumes. Refer to "To Create a File Volume or Segment Using the Create File Volume Panel" on page 35 for instructions.

4. **Enter the maximum audit log file size, from 1 to 1024 megabytes.**

The log file will grow from 0 megabytes to the specified maximum size before creating a new audit log file. The existing audit log files will not be removed. When the volume reaches the 90 percent threshold, alerts are sent and no more log files are written.

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

Audit Log Files

Audit log files are formatted using date/timestamps as well as the system host name. The current log file will be formatted as `YYYYMMDDhhmmss.not_terminated.hostname`.

The timestamps are in Greenwich Mean Time (GMT). For example, if the current log file was started on October 21, 2005, at 1:15 PM GMT on the Sun StorEdge 5210 NAS Appliance host `=testhost`, the file would be `20051021131500.not_terminated.testhost`.

Once a log file is closed, the name is converted using the same timestamp format. So, if the same log file in the above example reached its maximum size on October 30, 2005, at 7:35 PM GMT, the name would convert to `20051021131500.20051030193500.testhost`.

Audit log files have special attributes. In addition to having zero permissions, they are marked undeletable and immutable, which prevents them from being removed, renamed, or written to by anyone but the system itself. These attributes can be removed by the administrator using the `chattr` command.

Note – Currently, there is no graphical user interface (GUI) support for reading or removing audit logs.

Audited Events

Only a small number of events are audited: system startup, shutdown, disk partition creation and deletion, and volume creation and deletion.

These events are not configurable.

Reading Audit Logs

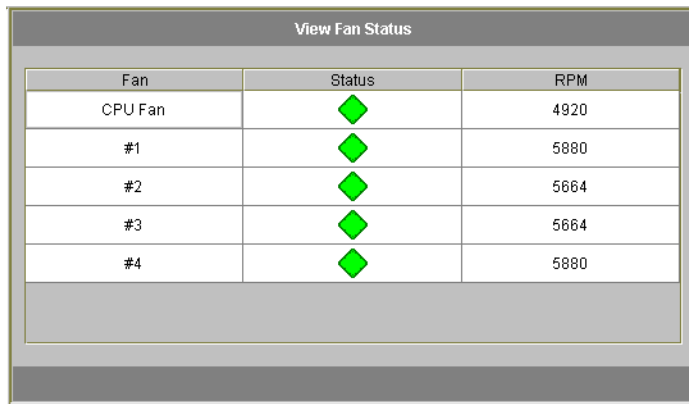
Since the audit logs are stored in binary format, they must be read using the `praudit` command. The `praudit` command converts the binary information in the audit logs into readable text.

Environmental Status

You can view information about the system fan, temperature, power supply, and voltage use.

▼ To View Fan Status

- To view the operational status and revolutions per minute (RPM) of all fans in the Sun StorEdge 5210 NAS Appliance head unit, select **Monitoring and Notification > View Environmental Status > View Fan Status** in the navigation panel.

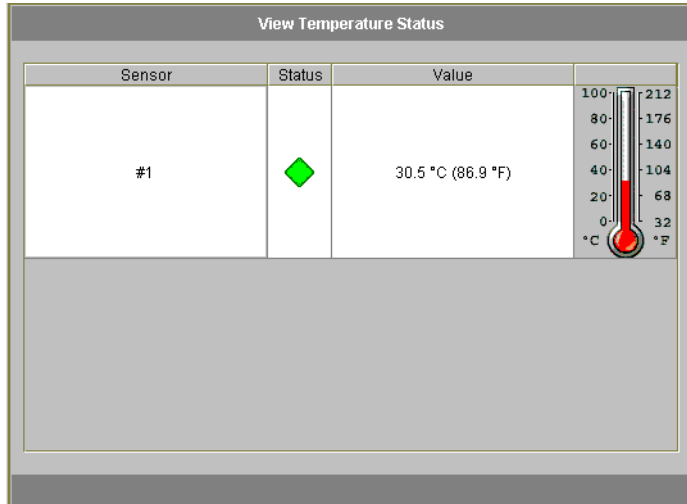


Fan	Status	RPM
CPU Fan	◆	4920
#1	◆	5880
#2	◆	5664
#3	◆	5664
#4	◆	5880

The screen shows the current status of each fan. A green diamond in the **Status** column indicates that the fan RPMs are normal. A red diamond indicates that the RPMs have exceeded the acceptable range. If the RPMs of any fan 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 22.

▼ To View Temperature Status

- To view temperature status, select **Monitoring and Notification > View Environmental Status > View Temperature Status** in the navigation panel.

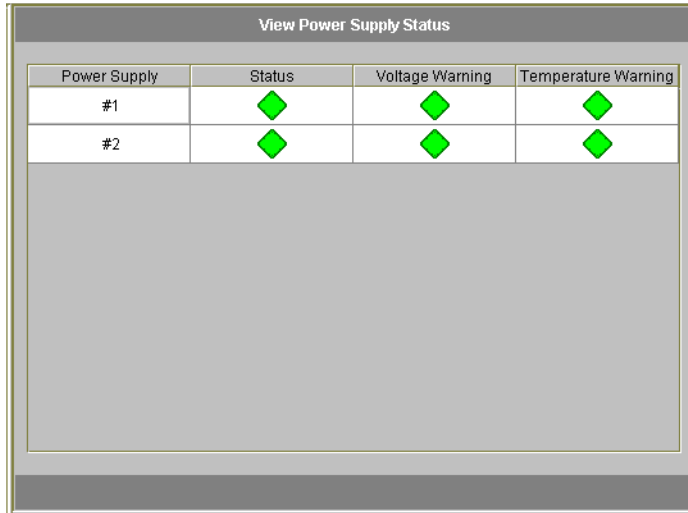


This screen displays the temperature of the sensors in the head unit. A green diamond in the Status column indicates that the unit is operating within the normal temperature range. A red diamond indicates that the temperature has exceeded the acceptable range. If the temperature rises above 55° Celsius (131° Fahrenheit), an email message is sent to the designated recipients. For more information on setting up email notification, see "Setting Up Email Notification" on page 22.

Note – You cannot change the temperature thresholds.

▼ To View Power Supply Status

- To display power supply status, select **Monitoring and Notification > View Environmental Status > View Power Supply Status** in the navigation panel.



















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

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 22.

▼ To View Voltage Status

- To display the current voltage readings, select **Monitoring and Notification > View Environmental Status > View Voltage Regulator Status** in the navigation panel.

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

See TABLE 10-3 for the acceptable range for each voltage.

TABLE 10-3 Acceptable Voltage Ranges

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

TABLE 10-3 Acceptable Voltage Ranges (*Continued*)

Voltage Value	Acceptable Range
Baseboard 5VSB (Standby)	4.781V to 5.156V
Baseboard 12V	11.50V to 12.56V
Baseboard 12V _{RM}	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 V _{ccp}	1.116V to 1.884V

Usage Information

You can view usage information for file volumes, network activity, system activity, and network ports.

▼ To View File Volume Usage

- To view the used and free space of file volumes in the system, 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 percent, an email is sent to designated recipients.

▼ To View Network Activity

- To display the number of I/O requests per second for all Sun StorEdge 5210 NAS Appliance clients, select **System Activity > View Networking Activity** from the navigation panel.

▼ To View System Activity

The Sun StorEdge 5210 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, select System Activity > View System Activity in the navigation panel.**

The system and network devices are listed in TABLE 10-4.

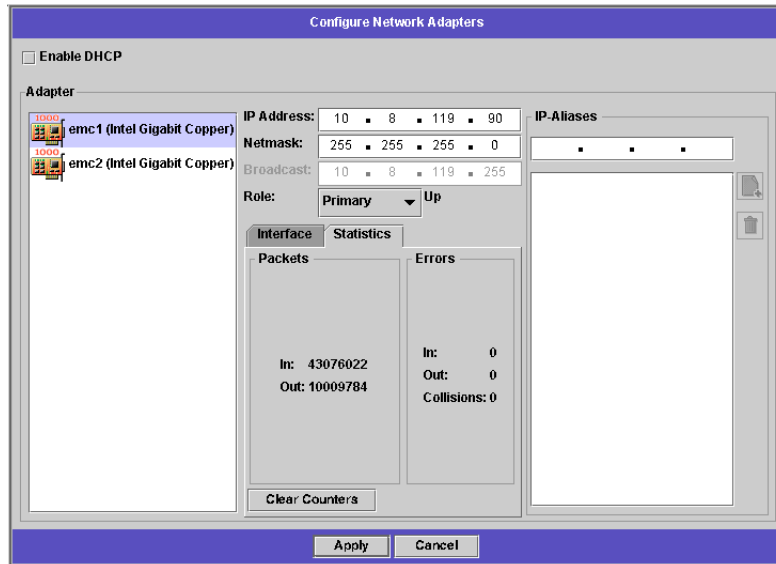
TABLE 10-4 System and Network Devices

Device Code	Device
CPU	Sun StorEdge 5210 NAS Appliance Central Processing Unit (CPU)
Memory	Sun StorEdge 5210 NAS Appliance system Random Access Memory (RAM)
Port Aggregation <i>x</i>	Port bond <i>x</i>
Controller <i>x</i>	RAID controller <i>x</i>
dac010 <i>xx</i>	Logical Unit Numbers (LUNs) <i>xx</i>
PORT <i>x</i>	Port <i>x</i>
Host Adapter <i>x</i>	SCSI host adapter <i>x</i> (for tape backup device)

▼ To View Network (Port) Statistics

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

The Viewing Network Statistics screen is displayed.



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. This 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 (Mbit/sec) at which data is transmitted over the network.
- MTU – Specifies the current maximum transmission unit (MTU) of the selected adapter. MTU is the largest frame length that can be sent on a physical medium. The highest possible MTU value is the default value of 1500. The minimum value you should 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 enables 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:

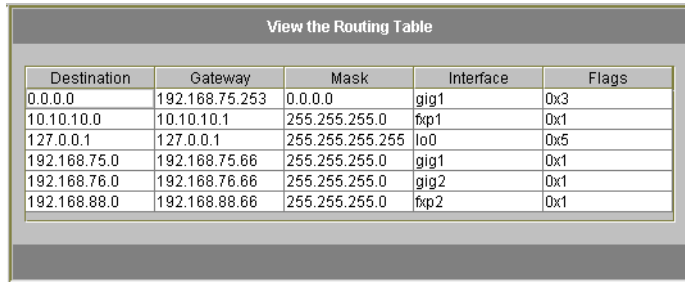
- 0x1 – Indicates that the route is usable.
- 0x2 – Indicates that the destination is a gateway.
- 0x4 – Indicates that the destination is a host entry.
- 0x8 – Indicates that the host or network is unreachable.
- 0x10 – Indicates that the destination was created dynamically.
- 0x20 – Indicates that 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.

▼ To Display Routes

To view the status of all routes in the local network, in the navigation panel, select **Network Configuration > View the Routing Table**.

The View the Routing Table Panel is displayed.



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

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 134 for more information.

Monitoring System Components

You can monitor uninterruptible power supply (UPS), controller, and mirror status.

UPS Monitoring

If you installed the unit with a UPS, you can monitor the UPS.

Note – You must connect the UPS to the Sun StorEdge 5210 NAS Appliance before you enable UPS monitoring. Otherwise, the monitoring system notifies you that there is a UPS failure. Also, the Sun StorEdge 5210 NAS Appliance does not support UPS management, only UPS monitoring. Refer to the *Sun StorEdge 5210 NAS Appliance Hardware Installation, Configuration, and User Guide* for a details about using the UPS.

UPS Monitoring Capability

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).

▼ To Enable UPS Monitoring

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

- In the navigation panel, select RAID > View Controller Information.

Viewing Mirroring Status

The Sun StorEdge 5210 NAS Appliance maintains a variety of network statistics for mirrored file volumes. These statistics are available on the active server and mirror server for each mirrored file volume.

▼ To View Mirror Statistics

1. From the navigation panel, select File Replicator > View Mirror Statistics.
2. Select the file volume you want from the Select Volume list.

The system displays the following 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 138.
- 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 have 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 have 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 have 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 have 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 maximum number of transactions that the buffer can hold.
 - 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 host name 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. The mirror status states include 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 unavailable.
- 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

You can view information about backup jobs, including the log, job status, and tape status.

▼ To View the Backup Log

- **In the navigation panel, select System Backup > Manage Backup Jobs > View 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 upward to view earlier backup events.

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

▼ To View Job Status

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

The 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.

▼ To View Tape Status

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

Note – You cannot view this data when a backup, restore, or head cleaning process is in progress.

System Maintenance

This chapter describes system maintenance functions.

The following topics are included:

- "Setting Remote Access Options" on page 141
- "Configuring FTP Access" on page 142
- "Shutting Down the Server" on page 143
- "File Checkpoints" on page 144
- "CATIA V4/V5 Character Translations" on page 150
- "Running a Head Cleaning" on page 151
- "Updating Sun StorEdge 5210 NAS Appliance Software" on page 152

Setting Remote Access Options

System security features include the ability to set remote access options. You can enable or disable network services used to remotely access the system. You can run the system in Secure Mode for maximum security or you can specifically enable certain remote access features such as Telnet, Remote Login, and Remote Shell.

The secure services are Secure Web Admin, which uses the Secure Socket Layer (SSL) over Hypertext Transfer Protocol (http), and Secure Shell (ssh).

▼ To Set Remote Access Security

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

2. Check the Secure Mode checkbox for maximum security. In secure mode you can enable only Secure Web Admin and Secure Shell by checking the associated checkbox.
3. If you are not using Secure Mode, 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, restart the server for the settings to go into effect. Refer to "Shutting Down the Server" on page 143.

Configuring FTP Access

File Transfer Protocol (FTP) is an Internet Protocol used to copy files between a client and a server. FTP requires that each client requesting access to the server must be identified with a username and password.

You can set up three types of users:

- Administrators who have the user name `admin` and use the same password used by GUI clients.

The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as `"/`.
- Users who have a user name and a password specified in the local password file or on a remote NIS, 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 log in with the user name `ftp` or its alias `anonymous`. A password is required but not authenticated. All guest users have access to all directories and files within the home directory of the `ftp` user.

Note – Guest users cannot rename, overwrite, or delete files; cannot create or remove directories; and cannot change permissions of existing files or directories.

▼ To Set Up FTP Users

1. In the navigation panel, select **UNIX Configuration > Set Up FTP**.
2. Check the **Enable FTP** checkbox.
3. Select the type of FTP access by checking the appropriate checkboxes:
 - Allow Guest Access enables access to the FTP server by anonymous users.
 - Allow User Access enables access to the FTP server by all users. This does not include the admin or root user.

Note – User names and passwords must be specified in the local password file or on a remote NIS, NIS+, or LDAP name server.

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

Note – A root user is a user with a user ID (UID) equal to 0 and the special Sun StorEdge 5210 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 enables you to shut down, halt, or reboot the server. (See "To Shut Down the System" on page 196 for information on shutting down the system using Telnet.)

▼ To Shut Down, Halt, or Reboot the Server

1. In the navigation panel, select **System Operations > Shut Down the Server**.
2. Select one of the following options:
 - None – Click this option if you do not want to shut down the server.
 - Reboot – Click this option to shut down 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.

- Halt This Head – Click this option to shut down this server (the one to which you are currently logged on). The other server remains online. To restart, you must manually power on the server.
- Reboot This Head – Click this option to shut down and restart this server (the one to which you are currently logged on). The other server remains online.

3. Click Apply.

File Checkpoints

A checkpoint, otherwise known as a “consistency spot” or “c-spot,” is a virtual read-only copy of a primary file volume. While the file volume remains in read/write operation, all data existing at the time the checkpoint was created remains available. Checkpoints are used to retrieve mistakenly modified or deleted files and to stabilize backups.

Note – A checkpoint is a virtual copy of the file volume that is stored in the same physical location as the volume itself. It is not an online backup. If the file volume is lost, so are all the checkpoints.

To use File Checkpoints, you enable checkpoints and create individual checkpoints or schedule checkpoints.

Creating File Checkpoints

You can choose whether to schedule a checkpoint or create one immediately. Refer to "Scheduling File Checkpoints" on page 145 for information on setting up a regular checkpoint schedule.

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

▼ To Create a New Checkpoint Manually

1. In the navigation panel, select **File Volume Operations > Edit Properties**.
2. From the Volume Name pull-down menu, select the volume for which you want to create a checkpoint.
3. Be sure there is a check mark in the **Enable Checkpoints** box.
If not, select the box and click **Apply**.
4. In the navigation panel, select **File Volume Operations > Configure Checkpoints > Manage Checkpoints**.
5. To create a new checkpoint, click **Create**.
6. From the pull-down menu, select the volume name for which you want to create a checkpoint.
7. Select one of the following checkpoint options:
 - **Auto Delete** – Select this option 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 5210 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 times and days, and the amount of time for which the checkpoint will be retained. The Keep time is expressed as the number of days plus the number of hours.

Adding a schedule line causes the system to automatically set up a checkpoint for the times and dates requested.

You can schedule a maximum of five checkpoints per volume. Multiple checkpoints may be specified per schedule.

An example of multiple checkpoints is shown below.

			Days	Hours AM	Hours PM	Keep	
Enabled	Description	SMTWTFS	M1234567890E	M1234567890E	M1234567890E	Days + Hours	
1.	Y	MTWTF5am5pm	-*****-	-----*-----	-----*-----	1	0
2.	Y	SunWed1pm	*--*---	-----	-*-----	0	12
3.	Y	MWFmidnight	-*-*-*	*-----	-----	0	3
4.	Y	Weekend	*-----*	*-----*	*-----*	0	6
5.	Y	FriEvery2hrs	-----*-	*-*-*-*-*	*-*-*-*-*	0	2

▼ 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. From the **Volume Name** pull-down menu, select the volume for which you want to add a checkpoint.
 - 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.**
3. **To add a checkpoint to the schedule, click Add.**
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. **In the Keep Days + Hours drop-down boxes, select the number of days and hours for which you want to retain the checkpoint.**
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 times 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 times of afternoon or night when the checkpoint is to be created.**

To select more than one item in this list, hold the Ctrl key while clicking additional items with the mouse.

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

▼ To Edit an Existing Checkpoint Schedule

1. **In the navigation panel, select File Volume Operations > Configure Checkpoints > Schedule Checkpoints.**

2. **Select the schedule line you want to edit, and click Edit.**

The information shown on this screen is identical to that in the Add Checkpoint Schedule dialog box, except that you cannot change the volume name.

3. **Edit the relevant information.**

For more information, see "To Add a Checkpoint to the Schedule" on page 146.

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

▼ 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.**

▼ To Rename a Checkpoint

1. **In the navigation panel, select File Volume Operations > Configure Checkpoints > Manage Checkpoints.**

2. **Select the checkpoint you want to rename, and click Rename.**

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

3. **Enter the new name for the checkpoint.**



Caution – If you rename an autodelete checkpoint to a common name, the checkpoint will no longer autodelete.

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

▼ To Remove a Checkpoint

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

Sharing File Checkpoints

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

▼ To Share File Checkpoints

1. In the navigation panel, select **Windows Configurations > Configure Shares**.
2. Click **Add**.
3. Type the new share name for the checkpoint in the **Share Name** box.
The share name is used to access the checkpoint from the network.
4. The **Mac Extensions** option is checked by default.
5. Click the **Volume Name** pull-down menu box and select the checkpoint volume from the list.
Checkpoint volumes have the `.chkpnt` extension.
6. Leave the **Directory** field blank.
7. If **ADS** is enabled and configured, type an **ADS** context in the **Container** text box.
8. Complete the following fields and options:
 - 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.

Note – These fields are unavailable if the system is configured for NT Domain mode.

9. Click **Apply**.

Notice the new checkpoint is listed as a share in the **Configure Share** panel.

Accessing File Checkpoints

Users can access checkpoints, allowing them to access the data that was current when the checkpoint was created.

▼ To Access a Checkpoint

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

Setting Up NDMP for Backups

The Network Data Management Protocol (NDMP) is an open protocol for network-based backup. NDMP architecture lets you use any NDMP-compliant backup administration application to back up your network attached storage (NAS) device. The Sun StorEdge 5210 NAS Appliance system supports NDMP network backups.

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

Note – Checkpoints must be enabled for volumes to be backed up by NDMP. Refer to "Creating File Checkpoints" on page 144.

▼ To Set Up NDMP

1. In the navigation panel, select **System Backup > Set Up NDMP**.
2. Select the NDMP NIC to be used for data transfer to the backup tape drive.

The gateway address is displayed for each port.

3. If the NDMP backup tape device is located on another network, select the port that connects to the correct gateway.
4. Click Apply.

CATIA V4/V5 Character Translations

The Sun StorEdge 5210 NAS Appliance interoperates with CATIA V4/V5 products (developed by Dessault Systemes).

CATIA V4 is a UNIX-only product, whereas CATIA V5 is available on both UNIX and Windows platforms. CATIA V4 may use certain characters in file names that are invalid in Windows. When CATIA customers migrate from V4 to V5, V4 files might become inaccessible in Windows if their file names contain invalid Windows characters. Therefore, a character translation option is provided for CATIA V4/V5 UNIX/Windows interoperability.

The translation table is shown in TABLE 11-1.

TABLE 11-1 CATIA Character Translation Table

CATIA V4 UNIX Character	CATIA V5 Windows Character	CATIA V5 Character Description
Curved open double quotation (not shown)	¨	Dieresis
*	¤	Currency sign
/	ø	Latin small letter O with stroke
:	÷	Division sign
<	«	Left-pointing double angle quotation mark
>	»	Right-pointing double angle quotation mark
?	¿	Inverted question mark
\	ÿ	Latin small letter Y with dieresis
	Broken bar (not shown)	Broken bar

CATIA V4/V5 interoperability support is disabled by default. You can enable the feature either manually through the command-line interface (CLI) or automatically after a system boot.

▼ To Enable CATIA Using the CLI

- **Issue the CLI command `load catia`. When using this method, you must re-enable CATIA support after each system reboot.**

▼ To Enable CATIA Automatically on Reboot

1. **Edit `/dvol/etc/inetload.ncf` to add the word `catia` on a separate line within the file.**
2. **Issue the following two CLI commands to restart the `inetload` service:**

```
unload inetload
load inetload
```

If CATIA V4/V5 support was successfully enabled, an entry similar to the following is displayed in the system log:

```
07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
```

Running a Head Cleaning

You can view information about the last head cleaning or set up the next head cleaning for the local tape device.

▼ To Run a Head Cleaning

1. **In the navigation panel, select `System Backup > Assign Cleaning Slot`.**
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 5210 NAS Appliance Software

Contact Sun Microsystems Technical Support to obtain the appropriate update files for your system configuration. Once you have the files, use the **Update Software** panel to update the Sun StorEdge 5210 NAS Appliance software.



Caution – Do not update system software or redundant array of independent disks (RAID) firmware when the RAID subsystem is in critical state, creating a new volume, or rebuilding an existing one.

▼ To Update Software

The following procedure requires you to reboot the system after the update process is complete. Rebooting the system requires all I/O to be stopped; therefore, plan to update the software during a planned maintenance period.

Note – In a cluster configuration, perform this procedure on both servers in the cluster.

1. In the navigation panel, select System Operations > Update Software.
2. In the Update Software panel, type the path where the update files are located.
If you need to look for the path, click Browse.
3. Click Update to start the process.

4. **When the update process is complete, click Yes to reboot, or click No to continue without rebooting.**

The update does not take effect until the system is rebooted.

Console Administration

The console is the alternative method to Web Administrator for managing the Sun StorEdge 5210 NAS Appliance. You can use a number of protocols, such as Telnet, Secure Shell (SSH), and RLogin to connect to the administrator console as long as the application you use has an American National Standards Institute (ANSI)-compatible terminal emulator. In this appendix, the Telnet protocol is used because it is readily available in Windows.

Note – You might need to change remote access security settings in order to access the command-line interface. Refer to "To Set Remote Access Security" on page 141 for remote access details.

This appendix includes the following topics:

- "Accessing the Console Administrator" on page 156
- "Console Menu Basics" on page 157
- "Viewing the Main Menu" on page 158
- "Configuration Backup" on page 158
- "System Management" on page 159
- "Managing Routes" on page 164
- "Name Services" on page 164
- "Managing the Server File System" on page 168
- "Managing Shares and Quotas" on page 171
- "Security" on page 176
- "Mirroring File Volumes" on page 183
- "Monitoring" on page 190
- "System Maintenance" on page 194

Accessing the Console Administrator

In this example the Windows Telnet Protocol is used. However, you can 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, type **cmd** and click **OK**.
4. At the command prompt, type **telnet *ipaddress***, where *ipaddress* is the IP address of the server, and press **Enter**.
5. If administrative access is password-protected, enter the password.

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

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

At this point, you can go directly to the main menu or you can access the command-line interface (CLI) to perform specific commands.

To access the main menu, press **Enter**.

▼ To Access the Command-Line Interface

1. At the connection prompt, type **admin** and press **Enter**.
2. Type the administrative password and press **Enter**.

The command line prompt appears. You can type a command or select menu to access the console's main menu.



Caution – Use commands carefully to avoid unintended results.

To return to the command line, press **Esc** from the main menu.

Console Menu Basics

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 the letter you need to select to perform the action.
- Use the spacebar to scroll through a list.

Key Descriptions

The keys used to edit screen fields are listed in the following table.

TABLE A-1 Active Screen Keys

Keys	Description
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. 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 spacebar to scroll through the extension lists.

▼ To Use the Menu

1. Choose a menu item by pressing the corresponding letter or number.
2. Press the spacebar to view more options under the Extension lists.

Configuration Backup

After you configure the system, you should create a backup of the configuration.



Caution – The system stores redundant copies of the configuration information, but you must make a backup copy in case of system failure.

▼ To Back Up the Configuration Information

In a cluster configuration, perform the following procedure on only one server. The configuration is automatically synchronized between servers; therefore, it is not necessary to create a backup of the configuration on each server.

1. Follow the instructions for "To Access the Command-Line Interface" on page 156.



Caution – Use commands carefully to avoid unintended results.

2. At the command line, enter `load unixtools`.
3. Enter `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

You can use the console administrator to perform system management tasks.

▼ To Configure TCP/IP

1. From the Configuration menu, select **Host Name & Network**.
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 Step 3 through Step 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**.

▼ To Modify the Administrator Password

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

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

Note – Always protect your system with a password.

3. If you selected **Yes, follow these steps in response to the prompts:**
 - a. Enter the password for administrative access, then type it again to confirm.
 - b. Select **7. Save changes to activate the new password.**

Controlling the Time and Date

Use the **Timezone, Time, Date** menu option to change time zone, time, and date set on the system. The real-time clock on the mainboard keeps track of local time.

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



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

▼ To Set the Time Zone, Time, and Date

1. From the **Configuration** menu, select **Timezone, Time, Date.**
2. Select the appropriate time zone, then press **Enter.**
3. Select **daylight savings time, Y or N.**

4. Type the new date, then press **Enter.**

The format is **YYYYMMDD**, where **YYYY** is the year, **MM** is the month, and **DD** is the day. For example, **20051001** equals October 1, 2005.

5. Type the current time, then press **Enter.**

The system uses a 24 hour clock.

6. Select **7. Save changes.**

Setting Time Synchronization

You can configure the system to synchronize its time with either the Network Time Protocol (NTP) or an RDATE server.

NTP is an Internet Protocol used to connect and synchronize the clocks of computers to a reference time source. Typical NTP configurations use multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

RDATE servers are normally present on UNIX systems and enable you to synchronize system server time with RDATE server time.

▼ To Set Up NTP

- 1. From the Extensions menu, select NTP Configuration.**
- 2. Select 1. Edit fields to configure NTP settings.**
- 3. Select Y. Yes to enable NTP.**
- 4. Follow these steps for each of the NTP servers you are configuring.**

You can configure up to two NTP servers.

- a. Select Y. Yes to enable the first NTP server.**
- b. Enter the name or IP address of the NTP server the Sun StorEdge 5210 NAS Appliance polls for the current time, then press Enter.**
- c. Choose the type of Authentication to use, either 0. none or 1. symmetric-key.**

Symmetric key authentication support lets the Sun StorEdge 5210 NAS Appliance verify that the NTP server is known and trusted by using a key and key ID. The NTP server and Sun StorEdge 5210 NAS Appliance must agree on the key and key ID to authenticate their messages.
- d. 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.

- 5. 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.

- 6. 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.

- 7. In the Broadcast Client Enabled field, select Y. Yes for the Sun StorEdge 5210 NAS Appliance to respond to server broadcast messages received on any interface.**

- 8. 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.

- 9. Select 7. Save changes.**

▼ To Set Up the RDATE Server and Tolerance Window

- 1. From the Extensions menu, select RDATE time update.**
- 2. Select 1. Edit fields.**
- 3. Enter the RDATE server name or IP address, and press Enter.**
- 4. Enter the tolerance and press Enter.**

If the Sun StorEdge 5210 NAS Appliance system time is different than RDATE server time by less than this number of seconds (+ or -), Sun StorEdge 5210 NAS Appliance system time is synchronized with RDATE server time. This check occurs every day at 11:45 p.m.

- 5. Select 7. Save changes.**

Setting Up Anti-Virus Protection

If you have an anti-virus scan engine running on your network, you can configure anti-virus protection on the system. For more detail about anti-virus protection, refer to "Using Anti-Virus Software" on page 53.

▼ To Enable Anti-Virus Protection

- 1. From the Extensions menu, select Anti-Virus Configuration.**
- 2. Select 1. Edit fields.**
- 3. In the AVA Enable field, enable anti-virus protection by specifying Yes.**

4. In the Scan mode field, select the scan mode.

Refer to “To Enable Anti-Virus Protection” on page 53 for details about scan mode options.

5. Specify the TCP/IP address of the scan engine to be used.

6. Specify the TCP/IP port number on which the ICAP server is to listen for connections; this is typically port 1344.

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

8. Specify the file types you want to include and exclude as well as any exempt clients, groups, or shares.

Specification	Description	Format
File Types Included	Each file type extension to be included. Leave blank to include all.	Three or fewer characters, comma-separated. May use ? for wildcard matching.
File Types Excluded	Each file type extension to be excluded from scanning.	Three or fewer characters, comma-separated. May use ? for wildcard matching.
Exempt Clients	Name or IP address of each client exempt from scanning.	Comma-separated.
Exempt Groups	Name of each Windows/NT or Windows Active Directory group (not UNIX group) exempt from scanning.	May include spaces, comma-separated.
Exempt Shares	Name of each CIFS share exempt from scanning. Note: administrative shares (X\$) are always exempt from scanning.	Comma-separated.

9. Select 7. Save changes.

Selecting a Language

You can specify the language for Network File system (NFS) and Common Internet File System (CIFS).

▼ To Select a Language

1. From the Extensions menu, select Language Selection.
2. Type the desired language then press Enter.

The languages that are supported are listed at the top of the screen.

Managing Routes

The routing table contains a list of network paths by which the system sends network packets to specified destinations. Each route entry consists of a destination address and a path. The destination is either a network or a host. The path is the gateway device through which the packet reaches its destination.

▼ To Manage Static Routes in the Local Network

1. From the Configuration menu, select Host Name & Network.
2. Select 2. Manage Routes.
3. Select 1. Add route, then select 1. Edit.
4. Select whether the route type is for a host, network, host through a gateway, or network through a gateway.
5. Enter the destination IP address, then press Enter.
6. Enter the path or gateway address used to connect the Sun StorEdge 5210 NAS Appliance with its destination, then press Enter.

The gateway device must connect to the same subnet as the Sun StorEdge 5210 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.

▼ To Set Up DNS, Dynamic 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 UNIX system with the `syslogd` utility on the network that can receive the Sun StorEdge 5210 NAS Appliance system log. All of these functions are set up on the same screen.

After the `syslogd` utility is set up, all log messages are sent to the selected server. This allows you to centralize a record of log messages from all the servers onto one system.

1. From the Configuration menu, select **DNS & SYSLOGD**.
2. Select **1. Edit fields**.
3. Select **Y. Yes to enable Domain Name Service (DNS)**.
4. Enter the IP address for the DNS server to be consulted first for name resolution, then press **Enter**.
5. Enter the IP address of the server to be consulted second for name resolution, then press **Enter**.
If you do not have a secondary DNS server, leave this field blank.
6. Enter the domain name of the DNS server, then press **Enter**.
7. Enter the maximum number of times the system should attempt a DNS query for each DNS server, then press **Enter**.
8. Enter the number of seconds of delay between attempts to query a DNS server, then press **Enter**.
9. To enable remote logging, select **Y. Yes**. If there is no `syslogd` server on the network, select **N. No** and skip to step 15.
This feature lets the Sun StorEdge 5210 NAS Appliance send log messages to a remote `SYSLOGD` server.
10. Enter the `syslogd` server name or IP address, then press **Enter**.
11. Select the appropriate facility, then press **Enter**. The facility identifies the application or system component generating the messages. Facilities include:
 - Kern – Messages generated by the kernel. These cannot be generated by any user processes.
 - User – Messages generated by random user processes. This is the default facility identifier if none is specified.
 - Mail – The mail system.

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

12. Select the types of system events you want to include in the Sun StorEdge 5210 NAS Appliance logs:

a. Select the appropriate event type.

b. Select Y. Yes to enable reporting of events of that type. Event types include the following:

- Emerg – Emergency messages. These messages are not distributed to all users. Emerg priority messages can be logged into a separate file for reviewing.
- Alert – Important messages that require immediate attention. These messages are distributed to all users.
- Crit – Critical messages not classified as errors, such as hardware problems. Crit and higher-priority messages are sent to the system console.
- Err – Any messages that represent error conditions, such as an unsuccessful disk write.
- Warning – Any messages for abnormal, but recoverable, conditions.
- Notice – Important informational messages. Messages without a priority designation are mapped into this priority message.
- Info – Informational messages. These messages are useful in analyzing the system.
- Debug – Debugging messages.

c. Press Enter to move to the next event type.

13. Select Y. Yes to enable Dynamic DNS updates.

These updates enable nonsecure dynamic updates to occur during bootup.

14. To enable secure updates, enter the name of a Windows user with whom the dynamic DNS client can verify updates, then press Enter.

This user must have administrative rights.

15. Enter the password of the Dynamic DNS user, then press Enter.

16. Enter Y. Yes to enable local logging.

17. Enter the log file path (directory) and file name in the Log File field.

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.

▼ To Enable NIS or NIS+

Note – Once Network Information Service (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.

1. From the Configuration menu, select NIS & NIS+.
2. Select 1. Edit fields.
3. Select Y. Yes to enable the Sun StorEdge 5210 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 5210 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.

▼ To Set Up Lookup Orders

You can choose which service is used first for user, group, and host lookup functions.

1. From the Configuration menu, select **Lookup orders**.
2. Select **1. Edit fields**.
3. Select the order for resolving user information (between NIS and NIS+), then press **Enter**.
4. Select the order for resolving group information (between NIS and NIS+), then press **Enter**.
5. Select the first, second, third, and last services for resolving host information, then press **Enter**.
6. Select **7. Save changes**.

Managing the Server File System

There are several procedures available through the console that let you manage the Server File System (SFS) volumes. The most common are as follows:

- Configuring drive letters
- Configuring a new disk volume
- Renaming a disk partition
- Deleting a disk volume
- Enabling and disabling quotas and checkpoints

Configuring Drive Letters

Drive letters are automatically assigned to file volumes available for sharing through Server Message Block (SMB)/CIFS. You can manually assign the drive letter mappings through the console, except for drive `C:`, which can only be assigned to `\cvol`.

It is possible to run out of drive letters, after which you may see the following log message:

```
No drive letter available
```

This message is for informational purposes only. The file system will be created but, to assign it a drive letter, you must reassign a drive letter that is currently used by another file system.

▼ To Manually Reassign a Drive Letter to a File Volume

1. From the Configuration menu, select Drive Letters.
2. Enter the drive letter you want to change, then press Enter.
3. Enter the file volume name you want to assign to the new drive letter, then press Enter.

You can only assign existing file volumes to drive letters.

4. Press Esc to exit this screen.

▼ To Create a New Disk Volume

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to configure.
3. Select 1. Edit.
4. Select 1. Create partition.
5. Select the partition type for the drive or press Enter to accept the default, for example, `sfs2` (primary volume) or `sfs2ext` (segment).
6. Enter the disk volume label, then press Enter.

The system will ask if you want to enable Compliance Archiving on this volume.

7. If you have a license for the Compliance Archiving software and want to create a compliance-enabled volume, press Y.



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

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.

▼ To Rename a Partition

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to rename.
3. Select 1. Edit.
4. Select 3. Rename.
5. Enter the new name of the partition and press Enter.

Note – Strict compliance-enabled volumes cannot be renamed.

▼ To Add 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 the volumes 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 spacebar to scan through them.

3. Type the number next to the partition you are changing.
4. Select 5. Segments.
5. Select 1. Add an extension segment.
6. Select the letter next to the extension drive you want.
7. Select 7. Proceed.

▼ To Delete a Disk Volume

Note – Mandatory enforcement compliance-enabled volumes cannot be deleted.



Caution – All data in the volume is lost when you delete a volume.

1. From the Configuration menu, select Disks & Volumes.
2. Enter the letter of the drive you want to configure.

Note – If you have more than 26 disk drives (disk volumes), press the spacebar to scan through them.

3. Select 1. Edit.
4. Select 8. Delete.
5. Enter the disk volume name and press Enter.
6. Select 7. Proceed with delete. Wait for the messages “Delete OK” and “Delpart OK”.
7. Press Esc to return to the Configure Disk menu.
8. Press Esc until you are back to the main menu.

Managing Shares and Quotas

You can manage shares and quotas using the console.

Setting Up 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 5210 NAS Appliance.

▼ To Set Up Shares

1. From the Extensions menu, select CIFS/SMB Configuration.

2. **Select A. Domain Configuration.**
3. **Enter a workgroup or domain name in the Domain field.**
4. **Define the domain scope, if applicable.**
5. **Enter a text description of the Sun StorEdge 5210 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 5210 NAS Appliance reboots.

Setting Up SMB/CIFS Autohome Shares

Autohome shares are temporary shares created when a user logs on to the system and removed when the user logs off.

The autohome share feature requires two configuration parameters, state and autohome path, defined as follows:

- The state parameter defines whether the feature is enabled or disabled. The environment variable `smb.autohome.enable` holds the current state of the feature; the value must be `yes` or `no`.
- The autohome path parameter defines the base directory path for the temporary shares. It is defined by the `smb.autohome.path` environment variable. For example, if a user's home directory is `/vol1/home/john`, then the autohome path should be set to `/vol1/home`. The temporary share will be named `john`. The user's home directory name must be the same as the user's logon name.

If the feature is disabled, the autohome path parameter is not relevant and will not be validated.

If the feature is enabled and the path is a zero length string, the configuration will be ignored. Otherwise, the path will be validated. If the autohome path parameter does not represent an existing directory path, an informational message will be written to the system log. For example, if the specified base path was `/vol1/home`, the log message would be as follows:

```
SMB autohome: /voll/home: no such directory
```

The log message is intended to inform the system administrator of the situation, but the configuration is still considered valid. The system will operate normally, but autohome shares will not be created. If the directory path is created at some later time, autohome shares will be added and removed, as required, from that point on.

▼ To Enable Autohome Shares

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select F. Autohome Setup.
3. Select 1. Edit fields.
4. Select Y. Yes to enable autohome shares.
5. Enter the autohome path.

The autohome path defines the base directory path for the shares. For example, if a user's home directory is `/usr/home/john`, then set the autohome path parameter to `/usr/home`. The temporary share is named `john`. The system assumes that the user's home directory name is the same as the user's logon name.

6. Select 7. Save changes.

▼ To Define a Share

After the SMB/CIFS setup is complete, you must define SMB/CIFS shares. Shares allow Windows users to access directories in the Sun StorEdge 5210 NAS Appliance.

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.
3. Select 8. Add a share.
4. Enter a share name.
5. Enter a path in the directory, in the form *volume/directory*.
6. Enter a comment about this directory, if applicable.
7. If your system is configured for Workgroup mode follow these steps:
 - a. In the Password Protection pull-down menu, select Yes or No.
If this is enabled, there is an option for either read/write or read-only.
 - b. Enter User ID, Group ID, and Umask.

8. Select 7. Save changes.

▼ 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 the previous section, "To Define a Share" on page 173.
7. Select 7. Save changes.

▼ To Delete a Share

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select E. Shares.
3. Enter the letter corresponding to the share you are deleting.
4. Select 8. Delete.

Setting Up Active Directory Service

When the Active Directory Service (ADS) is enabled and set up on this screen, the Sun StorEdge 5210 NAS Appliance automatically performs ADS updates.

▼ To Enable ADS Service

1. From the Extensions menu, select ADS Setup.
2. Select 1. Edit fields.
3. Select Y. Yes to let the ADS client publish Sun StorEdge 5210 NAS Appliance shares to ADS.

4. **Enter the Windows domain on which ADS is running.**
The Sun StorEdge 5210 NAS Appliance must also belong to this domain.
5. **Enter the name of a Windows user with administrative rights.**
The ADS client verifies secure ADS updates with this user.
6. **Enter the Windows administrative user's password.**
7. **In the User Container field, enter the ADS path for the Windows administrative user in LDAP DN notation.**
For more information see "To Enable ADS" on page 63.
8. **Enter the name of the local ADS site in the Site field.**
9. **Enter, in uppercase letters, the Kerberos realm name used to identify ADS.**
This is normally the ADS domain.
10. **Enter the host name of the Kerberos Key Distribution Center (KDC) server.**
This is usually the host name of the main domain controller in the ADS domain. You can leave this field blank if the ADS client or dynamic DNS client can locate the KDC server through DNS.
11. **Select 7. Save changes.**

Enabling and Disabling Quotas

Quotas track and limit the amount of disk space each user and group uses. You can turn the quota tracking function on and off. This function only enables and disables quotas. It does not set quota limits.

Note – Quota initialization takes several minutes, during which time the volume is locked and unavailable to users.

▼ To Enable or Disable Quotas

1. **From the Configuration menu, select Disks & Volumes.**
2. **Select the drive for which you are enabling quotas.**
3. **Select 1. Edit.**
4. **Select 4. Quotas on/off.**
5. **Select 1. Turn quotas on or 8. Turn quotas off.**

Security

You can set up groups and credential mapping to ensure security.

Configuring User Groups

The requirements for built-in local groups are different from those of a Windows NT system. For a complete description of user groups, see "Local Groups" on page 69.

▼ To Add a Group

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press 8. Add a Group to add a local group.
4. Type in the name of the group and press Enter.
5. Type in a description of the group, if applicable, and press Enter.
6. Press 7. Save changes to save the new group.

▼ 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 format *domain\username*.

The domain identifies the domain where the user name can be authenticated. For example, typing BENCHLAB\john identifies the domain BENCHLAB where the user john can be authenticated.

7. Press Enter.
8. Press 7. Save changes to save the new member.

▼ 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 Local Groups" on page 70.

▼ To Modify Local Group Privileges

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select B. Local Groups.
3. Press the letter of the group you want to modify.
4. Press 3. Privileges to change the privileges of the group members.
5. Press the letter of the privilege that you want to add or remove.
6. Press 7. Save changes to save the changes that you made.

User and Group Maps

For a complete description of user and group credentials, see "Mapping User and Group Credentials" on page 75.

▼ To Add a User Map

1. From the Extensions menu, select CIFS/SMB Configuration.

2. Select C. User Mapping.
3. Press 8. Add a map.
4. In the Account field, enter the domain and name of the NT user that you want to map to a UNIX user.
Use the format *domain\username*.
5. In the Name field, enter the name of the UNIX user that you want to map to the NT user.
6. Press 7. Save changes.

▼ To Edit a User Map

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select C. User Mapping.
3. Press the letter of the map that you want to edit.
4. Press 1. Edit Fields.
5. Type your changes and press Enter.
6. Press 7. Save changes.

▼ To Remove a User Map

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select C. User Mapping.
3. Press the letter of the user map that you want to delete.
4. Press 8. Delete.

▼ To Add a Group Map

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press 8. Add a map.
4. In the Account field, enter the domain and name of the NT group that you want to map to a UNIX group. Use the format *domain\username*.

5. In the Name field, enter the name of the UNIX group that you want to map to the NT group.
6. Press 7. Save changes.

▼ To Edit a Group Map

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press the letter of the group map that you want to edit.
4. Press 1. Edit Fields.
5. Type your changes and press Enter.
6. Press 7. Save changes.

▼ To Remove a Group Map

1. From the Extensions menu, select CIFS/SMB Configuration.
2. Select D. Group Mapping.
3. Press the letter of the group map that you want to delete.
4. Press 8. Delete.

Mapping and Securable Objects

This section details the interaction between user or group credential mapping and the securable objects within the system, such as, files and directories in the file system.

Objects residing on the system are classified according to the domain from which its security attributes were set. Objects that are created using the NFS protocol have only UNIX security attributes and thus are classified as UNIX objects. Objects created using the SMB protocol have both UNIX and Windows security attributes; they are classified as Windows objects. Although it is possible to allow objects to migrate from either domain to the other, as the security attributes are changed, a policy decision has been made that only one of the migrations will be allowed. A UNIX object becomes a Windows object when its security attributes are changed using SMB. By default, the security attributes of a Windows object cannot be changed using NFS. This is because Windows security is based on security descriptors, which cannot always be accurately represented using UNIX security attributes. Allowing a Windows object to become a UNIX object could potentially weaken the access control protecting the object.

Two mechanisms are provided to allow the attributes of a Windows object to be modified via NFS: the `ch smb` command and the `acl.override.allowed` environment variable.

If the `acl.override.allowed` is not present or is set to `no`, the default behavior will be applied; that is, the attributes of a Windows object cannot be changed via NFS.

If the `acl.override.allowed` environment variable is set to `yes`, UNIX commands, such as `chown`, `chgrp`, and `chmod`, will be permitted, according to the standard UNIX access rules. If the attributes of a Windows object are modified using NFS, the Windows security descriptor will be deleted, and the object will become a UNIX object.

The `ch smb` command can be used to remove a single Windows security descriptor or the entire Windows security descriptor database for a volume. To apply the `ch smb` command to an individual file or directory, you must specify the absolute path to that object. Note that `ch smb` does not perform recursive operations, so subdirectories or files contained within a directory will not be affected if the command is applied to a directory. The following examples illustrate how to use the `ch smb` command.

To delete the security descriptor and revert to the UNIX permissions on `/vol1/shared/bin/file.doc`, use the following command:

```
ch smb /vol1/shared/bin/file.doc
```

To delete all security descriptors on `/vol1` and revert all files to their UNIX permissions, use the following command:

```
ch smb /vol1
```

The `ch smb` command affects file security, so extra care should be taken when using this command. When a volume is specified, the `ch smb` command will issue a warning and prompt for confirmation before any action is taken.

No mapping is performed when a Windows user accesses a Windows object. Similarly, no mapping is performed when a UNIX user accesses a UNIX object. These are considered to be native access conditions. Also, because Windows objects have both Windows and UNIX security attributes, no mapping is required when a UNIX user accesses a Windows object, even though it is a nonnative access situation. This is a direct benefit of the design decision to choose one of the domains as the default mapping rather than creating an independent neutral mapping. Thus the only time that mapping is required is when a Windows user accesses a UNIX object. When a Windows user accesses a UNIX object, the object's UNIX security attributes are mapped to the Windows domain and the Windows security policy is applied.

Configuring the Host List

The console allows you to configure host information.

▼ To Add a Host

1. From the Configuration menu, select **Hosts**.
2. Type the new host name, then press **Enter**.
The system verifies that the host name does not already exist.
3. Press **Enter** to add the host.
4. Enter the new host IP address.
5. Select 7. Save changes.

▼ 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.

▼ 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.

▼ To Designate a Trusted Host

1. From the Access Control menu, select **Trusted Hosts**.
2. Type a host name, then press **Enter**.

Note – For you to add a trusted host, the host must exist on the host list or NIS.

The system verifies that the trusted host name does not already exist. If the trusted host exists, the host information is displayed. If the host is not trusted, the system displays a warning.

3. **Select 7. Add to list.**

The new trusted host is added, and the system displays the name at the top of the screen.

▼ **To Delete a Trusted Host**

1. **From the Access Control menu, select Trusted Hosts.**

2. **Type in the name of the trusted host you are deleting and press Enter.**

3. **Select 8. Delete.**

The trusted host is removed from the list.

Managing Volume Access

Once you save the changes, the existing NFS mounts from clients are updated to reflect the new parameters.

Do not allow any access, either read or write, to the cvol volume.

Note – Trusted hosts are automatically granted read/write access to file volumes regardless of the volumes' access settings.

▼ **To Manage Volume Access for NFS Clients**

1. **From the Access Control menu, select Volume Access.**

2. **Enter the letter corresponding to the volume to change its access.**

3. **Enter the number corresponding to the type of access you are assigning; read/write access, read-only access, or no access.**

Note – Hosts on the trusted list are allowed read/write access regardless of the volume access parameters.

4. **Select 7. Save changes.**

Locking and Unlocking the Console

You can use the console to disable or enable most of the main menu options, preventing unauthorized use of the console. You must set the administrative password to secure the console.

▼ To Lock the Console

1. From the Operations menu, select Lock Console.
2. Enter the administrative password.
3. Select Y (Yes).

▼ To Unlock the Console

1. From the main menu, select Unlock Console.
2. Enter the administrative password.
3. Select Y (Yes).

Mirroring File Volumes

This section describes how to mirror file volumes from a Sun StorEdge 5210 NAS Appliance active system to a Sun StorEdge 5210 NAS Appliance mirror system. For more information on mirroring, see Chapter 9.

Configuring Active and Mirror Servers

After the primary IP addresses have been configured on the active and mirror servers and you have designated the roles of the ports connecting the Sun StorEdge 5210 NAS Appliance mirror servers to one another, you can configure mirroring on the active and mirror servers using the console interface.

▼ To Configure a New Active Server With a New Mirror Server

1. From the Configuration menu, select Host Names and Network.
2. Select 1. Edit Fields.

3. If you have not done so already, configure the ports connected to a local network or subnet.

For more information about configuring TCP/IP using the console, see "To Configure TCP/IP" on page 159. For more information on configuring ports, see Chapter 5.

4. Assign the server name and IP address for the port used for the connection between the active and mirror systems.
5. In the Role field of the port used for the connection between the active and mirror servers, select Mirror.
6. Select Save to save your changes and return to the main menu.
7. Set up DNS and NIS/NIS+, if these services are available, and the Name Service lookup order.

For more information about setting up name services, see "Name Services" on page 164.

8. Open a Telnet window to the mirror system, and repeat Step 1 through Step 6

The network connections of the active and mirror systems are now configured. See the following section to continue.

▼ To Configure an Existing Active Server With a New Mirror Server

1. On the active server, in the Configuration menu, select Host Names and Network.
2. Select 1. Edit Fields.
3. Assign the server name and IP address for the port used for the connection between the active and mirror systems.
4. In the Role field of the port used for the connection between the active and mirror servers, select Mirror.
5. Open a Telnet window to the mirror system, and repeat Step 1 through Step 4
6. In the Telnet window of the active server, press Esc until you see the following command line:

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

7. Log in as the administrator and enter the following:

```
ping xxx.xxx.xx.xx
```

where xxx.xxx.xx.xx is the IP address of the mirror server.

8. Repeat step 7. on the mirror server, entering the IP address of the active server.

The network connections of the active and mirror systems are now configured. Continue by configuring file volumes for mirroring.

Configuring File Volumes

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

Note – Once you mirror a file volume, you cannot rename the file volume while maintaining the mirroring connection. You can only mirror file volumes equal to or larger than 1 gigabyte.

▼ To Set Up a File Volume for Mirroring

Follow these steps first on the active system and then on the mirror system.

1. **Create a small (for example, 32-MB) file volume named `SYS` before creating any other volumes.**

If you already have file volumes on the active system, this step is optional.

2. **From the Configuration menu, select Disks and Volumes.**
3. **Select the drive on which you want to create the new file volume.**
4. **Select Create & init partition. Then select 1. sfs2.**
5. **Enter `SYS` for the name, and 64 for the size in MB.**

This forces residence of the `/etc` directory and the Sun StorEdge 5210 NAS Appliance configuration files it contains on the `SYS` volume.

Do not create any other file volumes on the mirror system.

▼ To Mirror File Volumes

1. **Using Telnet, connect to the active system and enter the main menu.**
2. **In the Operations menu, select Licenses and select the letter corresponding to Mirroring.**
3. **Enter the activation key exactly as provided by Sun Microsystems.**
4. **Press Esc until you see the main menu.**
5. **In the Extensions menu, select Mirrors.**
6. **Select Add mirror to create a new mirror.**

7. **Select a file volume to be mirrored by pressing the corresponding letter.**
The file volume must be equal to or larger than 1 GB.
8. **Enter the host name of the mirror system.**
9. **Enter the private IP address, if necessary.**
This is the IP address used for the mirroring connection with the mirror server.
10. **Enter the alternative IP addresses in the Alt IP Address fields.**
11. **If accessing the mirror server requires an administrative password, enter it in the Remote admin password field.**
12. **Enter the size of the transaction buffer reserve, then press Enter.**
13. **Select 7. Proceed to add the mirrored file volume.**
When the mirror volume reaches an in sync state with the active volume, the mirror volume is mounted as read-only.

Note – There can be no I/O activity to the active server during initial mirror synchronization.

During and after the mirror creation process, the system displays the Mirror Creation screen.

14. **To view the status of the mirror, select A.**
15. **To edit the alternate IP addresses or administrator password, select 1. Edit.**

Setting Warning Thresholds

When the transaction buffer reserve fills and overruns, the mirror is “cracked.” This screen allows you to set the percentages at which warnings are issued. The default percentages are 70, 80, and 90 percent.

- ▼ **To Set the Threshold Percentages at Which Warnings Are Issued**
 1. **On the active system, in the Extensions menu, select Mirrors.**
 2. **Select 3. Threshold Config.**
 3. **Select 1. Edit to edit the percentages shown on this screen.**
 4. **Enter the desired percentages.**

5. In the Alert Silent Period field, enter the number of hours the system should wait before reissuing the same threshold warning
6. Select 7. Proceed.

Promoting a Mirrored File Volume

In the event that the active system fails, the mirror system provides high availability. To make a mirrored file volume available to network users, promote the file volume. You must first break the mirror by disconnecting the active-mirror connection between the active file volume and the mirrored file volume. Then promote the volume and configure the mirrored file volume access rights. Once you break the mirror and promote the mirrored file volume, the two file volumes are completely independent.

▼ To Promote a File Volume on the Mirror System

1. On the mirror system, view the status of the file volume by selecting **Disks & Volumes from the Configuration menu.**

An asterisk (*) appearing after the name of the mirrored file volume indicates that the file volume is currently mirrored.

Note – You should break the mirrored file volume from the mirror system only if the active system is unavailable. To promote a file volume when the active system is available, break the mirror from the active system, not from the mirror system.

2. In the Extensions menu, select **Mirrors.**
3. Select the letter corresponding to the mirrored file volume that you are breaking.
4. Select 8. Break.
5. When prompted to confirm the break, select **Y. Yes to continue.**
6. Press **Esc** to return to the main Mirrors screen.
7. In the Extensions menu, select **Mirrors.**
8. Select **1. Promote Volume.**
9. Select the letter corresponding to the file volume that you want to promote.
10. Select **7. Proceed to promote the file volume.**

It might take several minutes to complete this process. For a mirrored file volume to be promoted, it must have reached an In Sync state at least once.

11. When the system finishes promoting the file volume, press Esc to return to the main menu.
12. (Optional) To configure NFS file volume access, select Volume Access from the Access Control menu.
13. Set the access rights to the file volume by selecting its corresponding letter.
14. Choose Read/write, Read only, or None.
15. Select 7. Save changes to continue.

The volume has been promoted. To reestablish a mirror, see the following section, "Reestablishing a Mirror" on page 188.

Reestablishing a Mirror

This procedure describes how to reestablish a mirror when the active server has failed and you have promoted the file volume on the mirror server. The promoted file volume is now the most up-to-date version and functions completely independently of the out-of-date file volume on the active system. To recreate the mirror, mirror the up-to-date file volume back to the active server and then mirror the file volume back to the mirror server as it was originally.

Note – If you have not promoted the mirrored file volume, do not follow these instructions. The active system automatically brings the mirror back to an In Sync state when it is back online.

In the examples that follow, Server 1 is the active server and Server 2 is the mirror server.

Reestablishing a mirror includes the following steps:

1. Breaking the mirror on Server 1
2. Deleting the out-of-date file volume on Server 1
3. Mirroring the up-to-date file volume from Server 2 back to Server 1
4. Change roles, making Server 1 active again and Server 2 the mirror server.

When the active server is brought online, it might attempt to reestablish the mirror. Therefore, you must break the mirror on Server 1.

▼ To Break the Mirror on Server 1

1. On Server 1, in the Extensions menu, select **Mirrors**.

2. Select the letter corresponding to the mirrored file volume.
3. Select 8. Break.
4. Select Y. Yes to confirm breaking the mirror.

▼ To Delete the Out-of-Date File Volume on Server 1

1. Press Esc to return to the main menu.
2. In the Configuration menu, select Disks & Volumes.
3. Select the number corresponding to the mirrored file volume.



Caution – Before completing the following step, be sure you are deleting the out-of-date file volume on Server 1. Also, be sure that the up-to-date file volume on Server 2 is verified and promoted first.

4. Select 8. Delete.
5. Enter the file name of the out-of-date file volume.
6. Select 7. Proceed with delete to delete the out-of-date file volume.

▼ To Mirror the Up-to-Date File Volume on Server 2 Back to Server 1

1. On Server 2, in the Extensions menu, select Mirrors.
2. Select 8. Add mirror.
3. Select the letter corresponding to the file volume that you are mirroring.
4. Enter the private host name of Server 1.
5. Enter the private IP address, if necessary, and the administrator password.
6. Enter the transaction buffer reserve.

For more information, see "To Mirror File Volumes" on page 185.

7. Select 7. Proceed.
8. During the mirror creation process, select the letter corresponding to the new mirrored file volume.

When the mirror reaches an In Sync state, an identical copy of the file volume exists on both Server 1 and Server 2. See the following sections to continue.

▼ To Change Roles

Note – Make sure the volumes are 100 percent in sync before changing roles.

1. **From the main menu, select the Mirror option on Server 1.**
2. **Select the desired volume by pressing the appropriate letter.**
For example, press A to select the cv011 file volume.
3. **From the Mirror Status menu, select the Change Role option.**
4. **Select Yes to confirm.**

Monitoring

You can use the console to perform monitoring functions.

Configuring SNMP

The SNMP menu lets you send messages to a remote Simple Network Management Protocol (SNMP) monitor, as well as modify the community string, contact information, and the location of the SNMP monitor.

▼ To Configure SNMP

1. **From the Extensions menu, select SNMP Configuration.**
Public is the default community name. You can enter any name you want.
2. **Select 1-5. Edit a Trap Destination to add, edit, or delete a trap destination, 6. Edit Community to edit the community string, 7. Edit Contact to edit contact information, or 8. Edit Location to edit the location of the remote SNMP monitor.**
3. **Select Y. Yes to save your changes.**

Configuring Email Notification

When there is a problem with your system, Sun StorEdge 5210 NAS Appliance sends email messages to specific recipients.

Note – You must configure DNS for email notification to function properly.

▼ To Configure Email Notification

1. From the **Extensions** menu, select **EMAIL Configuration**.
2. Select **1. Edit fields**.
3. Type the information requested for each field. Press **Enter** to move between fields.
 - SMTP Server – The mail server to which all mail is directed. 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 – The email addresses of the four people automatically notified in case of a problem.
 - Notification Level – The level a problem must be at before the recipients are notified through email. Select one of the following:
 - Errors – Notifications sent only for errors
 - Errors and warnings – Notifications sent for errors and low priority warnings
 - None – No notifications sent
4. Select **7. Save changes** to save the current configuration.
 5. Press **Esc** to return to the main menu.

Viewing System Information

You can view system information from the console.

▼ To View Server Status

1. From the **Operations** menu, choose **Activity Monitor**.

The Activity Monitor screen lists the following information:

- Volume – The first 22 file volumes
- Use% – The amount of space used on the volume
- Reqs – The number of requests processed for the volume in the last 10 seconds
- Device – The name of the device
- Load – The percentage of CPU load

- Peak – The highest usage per second in the last 10 minutes
- Client – The name or address of the user
- Reqs – The number of requests processed for the volume in the last 10 seconds

2. Press Esc to return to the main menu.

▼ To View the System Log

- From the Operations menu, select Show Log.

The log displays two types of entries:

- **System Startup Log Entries** – Reports device configurations, volumes, and other pertinent information.
- **Normal Operation Log Entries** – Reports device errors, security violations, and other routing status information. The release number and software serial number are listed last.

▼ To View Port Bonding

1. From the Configuration menu, select Host Name & Network.
2. Press the spacebar to scroll to the next page.

The bond1 column shows the first port bond. The input/output information in this column is the sum of the input/output information for the two ports that you bonded.

▼ To View the Checkpoint Analysis

1. From the Configuration menu, select Disks & Volumes.
2. Type the letter corresponding to the drive that you are configuring.
3. Select Change/Delete *volume-name*.
4. Select 6. Checkpoints.
5. Select 3. Analysis. Scroll through the analysis using the spacebar.
6. Select 0. End Analysis to exit this screen.

▼ To View the Status of a Mirrored File Volume

1. On the active system, select Mirrors from the Extensions menu.
2. Select the mirrored file volume.

There are three sections of the status screen:

- The first line displays the mirror state information, including file volume name, mirror state, a progress indicator, and a status message. There are ten mirror states:
 - ERR – An error has occurred.
 - NEW – A new mirror is being created.
 - INIT – The mirror buffer is being initialized.
 - MKPT – Disk partitions are being created on the mirror system.
 - RDY – The system is ready and waiting for the other system to be ready.
 - DOWN – The network link is unavailable.
 - CRK – The mirror is cracked.
 - RPL – The replication phase is occurring.
 - OOS – The mirror is out of sync.
 - SYNC – The mirror is in sync.

The progress indicator displays a progress percentage of activity within each state. A status message also gives a short text message describing the mirror status.

- The second line displays the condition of the transaction buffer reserve. The information displayed here is the maximum number of transactions the buffer can hold, the next transaction ID, the sync transaction ID, the head transaction ID, and an In Sync percentage indicator describing the state of synchronization between the active and mirror systems.

On the active system, the information is as follows:

- The next xid (next transaction ID) identifies the next transaction of the file system.
- The sync xid (sync transaction ID) identifies the last transaction that was transferred to the mirror system.
- The head xid (head transaction ID) identifies the last transaction that was acknowledged by the mirror system.
- When the In Sync percentage indicator is 100 percent, the mirror system has a complete copy of the active system. If the In Sync percentage indicator displays 0 percent, then the mirror is cracked and the active server automatically performs a block by block resync. While the mirror state is in the Out Of Sync state, the mirror volume is volatile.

On the mirror system, the information is as follows:

- The next xid (next transaction ID) identifies the next transaction that is expected from the active system.
- The sync xid (sync transaction ID) identifies the last transaction that was scheduled to be written to disk.

- The head xid (head transaction ID) identifies the last transaction that was acknowledged on disk.
- When the In Sync percentage indicator is 100 percent, all mirror transactions have been written to disk, and the mirror system volume is an exact copy of the active system volume.

3. To edit the alternate IP addresses or administrator password, select 1. Edit.

4. Edit the fields, then select 7. Proceed to save your changes.

5. To see network statistics on the mirrored file volume, select 2. Statistics.

The screen displays the statistics for the active system, including the number of transactions into the active file volume (IN) and out of the active system to the mirrored file volume (OUT). The screen shows the average, minimum, and maximum transactions per second (t/s) for each.

The system displays the amount of free space remaining in the transaction buffer reserve (Buffer), along with the fill rate. If the fill rate is greater than zero, you should check to make sure that all network links are functioning properly. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. When the buffer overruns, the mirror is “cracked.”

▼ To View Network Statistics for All Mirrored File Volumes

1. On the active system, select Mirrors from the Extensions menu.

2. Select 2. Network Statistics.

The screen displays the total number of request control blocks (RCBs) sent, the number of RCBs sent per second, and the average size of the RCBs, as well as their average response time and transfer rate.

3. Select 1. Reset to restart this display.

System Maintenance

There are several system maintenance and setup functions that can only be performed from the console. These are described in the following section:

- “Configuring FTP Access” on page 195
- “Mounting File Systems” on page 196

These sections describe additional tasks can be performed from the console administrator as well as from the Web Administrator:

- "Shutting Down the System" on page 196
- "Scheduling File Checkpoints" on page 197
- "Configuring Backup" on page 197
- "Configuring the Compliance Archiving Software" on page 198
- "Configuring System Auditing" on page 199

Configuring FTP Access

File Transfer Protocol (FTP) is an Internet protocol used to copy files between a client and a server. FTP requires that each client requesting access to the server be identified with a user name and password.

You can set up three types of users:

- Administrators who have the user name `admin` and use the same password used by GUI clients.

The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as `"/`.

- Users who have a user name and a password specified in the local password file or on a remote NIS or NIS+ name server.

The user has access to all existing directories and files within the user's home directory. The home directory is defined as part of the user's account information and is retrieved by the name service.

- Guests who log in with the user name `ftp` or its alias `anonymous`. A password is required but not authenticated. All guest users have access to all directories and files within the home directory of the `ftp` user.

Note – Guest users cannot rename, overwrite, or delete files; cannot create or remove directories; and cannot change permissions of existing files or directories.

▼ To Set Up FTP Access

1. **From the Extensions menu, select FTP Configuration.**
2. **Select 1. Edit Fields.**
3. **Select Y. Yes to enable FTP or N. No to disable it.**

If FTP service is enabled, the FTP server will accept incoming connection requests.

4. **In Allow guest access, select Yes to enable access to the FTP server by anonymous users or No to disable access.**

5. In **Allow user access**, select **Yes to enable access to the FTP server by all users or No to disable access**.

This does not include the `admin` or `root` user.

Note – User names and passwords must be specified in the local password file or on a remote NIS or NIS+ name server.

6. In **Allow admin access**, select **Yes to enable root access to those in possession of the Sun StorEdge 5210 NAS Appliance administrative password (use with caution) or No to disable access**.

Note – A root user is a user with a user ID (UID) equal to 0 and the special Sun StorEdge 5210 NAS Appliance user `admin`.

7. In **Enable logging**, select **Yes to enable logging or No to disable logging**.
8. If you enable logging, specify the log file name in **Log filename**.
9. Select 7. **Save changes**.

Mounting File Systems

After multiple continuous reboots, one or more file systems may become unmounted. To mount the file systems, issue the following command:

```
mount -f volume_name
```

Shutting Down the System

The Sun StorEdge 5210 NAS Appliance system is designed for continuous operation, but if you need to shut down the system, you must do it from the Web Administrator, the console, or the LCD panel.

▼ To Shut Down the System

1. From the **Operations** menu, select **Shutdown**.
2. Select the desired option by typing the appropriate letter option.
 - R. Reboot – Type “R” to reboot the system
 - H. Halt – Type “H” to halt the system.

- P. Boot Previous Version 4.x.xx.xxx – Type “P” to reboot the system using the available previous OS version. This option is available on systems that have more than one OS version installed.
- ESC – Press the Esc key to cancel and return to the main menu.

If you choose to reboot, halt, or boot with the previous OS version, the server reboots or turns off after all the delayed writes to disks are completed.

Scheduling File Checkpoints

A checkpoint is a virtual read-only copy of a primary file volume. See "File Checkpoints" on page 144 for detailed information about checkpoints.

▼ To Schedule Checkpoints

1. From the Configuration menu, select Disks & Volumes.
2. Select the drive for which you are scheduling checkpoints.

Note – If you have more than 26 drives (disk volumes), press the spacebar to scan through them.

3. Select 1. Edit.
4. Select 6. Checkpoints.
5. Follow the prompts at the bottom of the screen, pressing Enter to move through the fields.
6. When you have entered all checkpoint information, select 7. Save changes.

Configuring Backup

To back up system volumes, you must first add a backup job, then schedule or run it. Be sure the backup device is online before proceeding.

Note – Checkpoints must be enabled for volumes to be backed up by Network Data Management Protocol (NDMP). Refer to "Creating File Checkpoints" on page 144.

▼ To Set Up NDMP

1. From the Extensions menu, select NDMP Setup.
2. Select the Network Interface Card (NIC) port used for data transfer to the backup tape drive, and press Enter.

All available ports are shown below this field.

3. Select a spare volume path, for example `/vol_ndmp`, of at least 2 GB for saving NDMP log and data files.

You should use a separate file volume for this, apart from the volumes that are scheduled for backup.

4. Save changes.

Configuring the Compliance Archiving Software

If you have purchased, activated, and enabled the Compliance Archiving Software option (see "To Activate an Option" on page 101), there are additional settings you can establish using the CLI.



Caution – Use commands carefully to avoid unintended results.

▼ To Change the Default Retention Period

1. Follow instructions for "To Access the Command-Line Interface" on page 156.
2. At the command line, enter `fsctl compliance volume drt time`

where *volume* is the name of the volume for which you want to set the default retention time, and *time* is the duration of the default retention period, in seconds.

To set the default retention to "permanent," use the maximum allowable value, 2147483647.

▼ To Allow Windows Clients to Use the Compliance Archiving Functionality

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.

1. Follow instructions for "To Access the Command-Line Interface" on page 156.
2. At the command line, enter:
`fsctl compliance wte on`

Configuring System Auditing

System auditing is a service that allows you to audit particular system events by storing records of those events in log files. For more details about system auditing, refer to "System Auditing" on page 125.

▼ To Configure System Auditing

1. From the Extensions menu, select System Audit Configuration.
2. Select 1. Edit fields.
3. Enable auditing and specify the path for the audit log and the maximum file size for the log file.
4. Select 7. Save changes.

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 5210 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 5210 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. Email notification and the system log include the time of the event.

Sun StorEdge 5210 NAS Appliance Error Messages

The following sections show error messages for the Sun StorEdge 5210 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	AC Power Failure: AC power failure. System is running on UPS battery. Action: Restore system power. Severity = Error	EnvUpsOn Battery	U20 on battery	UPS: AC power failure. System is running on UPS battery.
Power Restored	AC power restored: AC power restored. System is running on AC power. Severity = Notice	EnvUpsOff Battery	U21 power restored	UPS: AC power restored.
Low Battery	UPS battery low: UPS battery is low. The system will shut down if AC power is not restored soon. Action: Restore AC power as soon as possible. Severity = Critical	EnvUpsLow Battery	U22 low battery	UPS: Low battery condition.
Normal Battery	UPS battery recharged: The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.
Replace Battery	Replace UPS Battery: The UPS battery is faulty. Action: Replace the battery. Severity = Notice	EnvUps Replace Battery	U23 battery fault	UPS: Battery requires replacement.
UPS Alarms - Ambient temperature or humidity outside acceptable thresholds	UPS abnormal temperature/humidity: Abnormal temperature/humidity detected in the system. Action: 1. Check UPS unit installation, OR 2. Contact technical support. Severity = Error	EnvUps Abnormal	U24 abnormal ambient	UPS: Abnormal temperature and/or humidity detected.

TABLE B-1 UPS Error Messages (Continued)

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Write-back cache is disabled.	<p>Controller Cache Disabled: Either AC power or UPS is not charged completely. Action: 1 - If AC power has failed, restore system power. 2 - If after a long time UPS is not charged completely, check UPS. Severity = Warning</p>		Cache Disabled	write-back cache for ctrl <i>x</i> disabled
Write-back cache is enabled.	<p>Controller Cache Enabled: System AC power and UPS are reliable again. Write-back cache is enabled. Severity = Notice</p>		Cache Enabled	write-back cache for ctrl <i>n</i> enabled
UPS is shutting down.	<p>UPS shutdown: 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>UPS failure: Communication with the UPS unit has failed. Action: 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR 2. Check the UPS unit and replace if necessary. Severity = Critical</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 percent.

TABLE B-2 File System Errors

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
File System Full	File system full: File system <name> is xx% full. Action: 1. Delete any unused or temporary files, OR 2. Extend the partition by using an unused partition, OR 3. Add additional disk drives and extend the partition after creating a new partition. (Severity=Error)	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is xx%.

RAID Subsystem Errors

Table B-3 displays events and error messages for the Sun StorEdge 5210 NAS Appliance.

TABLE B-3 RAID Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
LUN Failure	RAID LUN failure: 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	RaidLunFail	R10 Lun failure	RAID LUN <i>N</i> failed and was taken offline. Slot <i>n</i> is offline. (Severity=Error)
Disk Failure	Disk drive failure: Disk drive failure. Failed drives are: Slot no., Vendor, Product ID, Size Severity = Error	RaidDiskFail	R11 Drive failure	Disk drive failure. Failed drives are: Slot#, Vendor, Product ID, Size (Severity=Error)
Controller Failure	RAID controller failure: RAID controller <i>N</i> has failed. Action: Contact technical support. Severity = Error	RaidController Fail	R12 Ctlr failure	RAID controller <i>N</i> failed.

IPMI Events

Sun StorEdge 5210 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 5210 NAS Appliance Hardware Installation, Configuration, and User Guide*.

Table B-4 describes the IPMI error messages for the Sun StorEdge 5210 NAS Appliance.

TABLE B-4 IPMI Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Fan Error	Fan Failure: Blower fan <i>xx</i> has failed. Fan speed = <i>xx</i> RPM. Action: The fan must be replaced as soon as possible. If the temperature begins to rise, the situation could become critical. Severity = Error	envFanFail trap	P11 Fan <i>xx</i> failed	Blower fan <i>xx</i> has failed!
Power Supply Module Failure	Power supply failure: The power supply unit <i>xx</i> has failed. Action: The power supply unit must be replaced as soon as possible. Severity = Error	envPowerFail trap	P12 Power <i>xx</i> failed	Power supply unit <i>xx</i> has failed.
Power Supply Module Temperature	Power supply temperature critical: The power supply unit <i>xx</i> is overheating. Action: Replace the power supply to avoid any permanent damage. Severity = Critical	envPowerTemp Critical trap	P22 Power <i>xx</i> overheated	Power supply unit <i>xx</i> is overheating.

TABLE B-4 IPMI Error Messages (Continued)

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Temperature Error	<p>Temperature critical: Temperature in the system is critical. It is xxx Degrees Celsius. Action: 1. Check for any fan failures, OR 2. Check for blockage of the ventilation, OR 3. Move the system to a cooler place. Severity = Error</p>	envTemperatureError trap	P51 Temp error	The temperature is critical.
Primary Power Cord Failure	<p>Power cord failure: The primary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error</p>	envPrimaryPowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
Secondary Power Cord Failure	<p>Power cord failure: The secondary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error</p>	envSecondaryPowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

Compliance Archiving Software API

The Sun StorEdge 5210 NAS Appliance product supports compliance data storage as a license key enabled software extension called “Compliance Archiving Software.”

The Compliance Archiving Software is available in a stringent form (referred to as “mandatory enforcement”) and in a less stringent form (referred to as “advisory enforcement”). For overview information about the Compliance Archiving Software, refer to “Compliance Archiving Software” on page 113.

This appendix is a technical overview of the features and programming interface for the Compliance Archiving Software with mandatory enforcement.

Note – Proper operation of the Compliance Archiving Software requires the correct physical configuration of the Sun StorEdge 5210 NAS Appliance system hardware.

Note – To ensure the strongest possible enforcement of your data retention policies, you should also provide for the physical security of your Sun StorEdge 5210 NAS Appliance system. Software-controlled data retention can be no stronger than the physical safeguards used to control access to the system’s hardware.

Compliance Features

The Compliance Archiving Software provides storage-level guarantees regarding the accuracy, integrity, and retention of files. 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 Network Files System (NFS) and Common Internet File System (CIFS) protocols. When an application designates a file as WORM, the file becomes permanently immutable. WORM files cannot be modified, extended or renamed, regardless of the identity or privileges of the client or user attempting the operation. In addition, WORM files can only be deleted in accordance to the file retention rules described below.

Note – Although these files are called "WORM," in keeping with common parlance for nonrewritable, nonerasable storage, it would be more accurate to call them "permanently read-only." The Sun StorEdge 5210 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 can be extended, but never decreased. A new retention period can 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 5210 NAS Appliance (NFS and CIFS). In particular, the Sun StorEdge 5210 NAS Appliance overloads existing file attributes to indicate the WORM status of a file and the end of its retention period. This simplifies the porting of existing document and record management applications because these metadata fields can be set and viewed using standard client APIs and utilities.

Compliance Volumes

Volumes must be designated as compliance-enabled at the time they are created; existing volumes cannot be converted into compliance volumes. It is possible to have multiple volumes on a single Sun StorEdge 5210 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 of a file's permission mode to 4000. Client applications or users can invoke this WORM trigger using the `chmod` command or system call. On receiving this request, the Compliance Archiving Software converts the target file into a WORM file by doing the following:

- Setting the setuid bit

- Clearing any write bits that are set on the file
- Retaining any read access bits on the file

Note – Executable files cannot be made into WORM files. For files created from Windows clients, this means that a file cannot be made into a WORM file if its access control list (ACL) has any access control entries (ACEs) granting execute permission on the file.

In the following example, a file with an access mode of 640 is converted to a WORM file. After the WORM trigger is issued, the file's access mode is 4440.

```
$ ls -l testfile
-rw-r----- 1 smith  staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr----- 1 smith  staff      12139 Dec  2 13:18 testfile
```

The Compliance Archiving Software uses this WORM trigger because it is an operation that is unlikely to be used by existing applications.

The WORM trigger for Windows clients is setting of both the read-only and the system bits on a file. The WORM trigger sets the file's read-only bit, but does not change its system bit.

After a file becomes WORM, it cannot be changed back. From Windows clients, the read-only bit cannot be cleared and the system bit cannot be changed. From UNIX clients, the `setuid` bit cannot be cleared, nor can execute or write permissions be added to the file's access mode.

Compliance-enabled volumes translate these WORM settings between CIFS and NFS. For example, if a UNIX client views a WORM file created by a Windows client, it sees a WORM access mode as described above.

Behavior of WORM Files

WORM files cannot be modified, overwritten, or extended. Any attempt to write to a WORM file will fail and return an error regardless of the client user's identity and access privileges.

Neither the owner of a WORM file nor a user with administrative privileges (even root privileges) can modify a WORM file. WORM files cannot be renamed or changed back to regular (non-WORM) files.

Metadata of WORM Files

The Compliance Archiving Software doesn't allow metadata that contains, protects, describes, or names client data to be modified. Only a restricted subset of metadata fields are allowed to change, depending on operating system, as shown in TABLE C-1.

TABLE C-1 WORM File Metadata That Can and Cannot Be Modified

Operating System	Can	Cannot
UNIX	<ul style="list-style-type: none">• Set or clear read permission bits• Change file and group owner	<ul style="list-style-type: none">• Enable write and execute bits• Clear <code>setuid</code> bit• Modify size or modification time (<code>mtime</code>)
Windows	<ul style="list-style-type: none">• Set or clear read permission bits• Change archive bit• Create and modify access control lists (although a WORM file can never be modified, regardless of ACL settings)	<ul style="list-style-type: none">• Change the read-only, system, or hidden bits• Modify size or modification time (<code>mtime</code>)

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 path name 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 of a file's `atime` value 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 of 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 through their local system call interface. These calls invoke the client NFS implementation, which translates system calls into standard NFS protocol requests. Because compliance-enabled file systems behave differently than standard NAS file systems, there are corresponding differences in the behavior of the client system calls.

This section describes the standard UNIX system calls that behave differently when a client executes them on a compliance-enabled Sun StorEdge 5210 NAS Appliance share. System calls not listed here behave as normal.

It is important to remember that the interfaces to the Sun StorEdge 5210 NAS Appliance are the NFS and CIFS file access protocols. Thus, this section incorporates both the compliance-related behavior of the Sun StorEdge 5210 NAS Appliance in response to standard protocol requests, and the mapping from system calls to NFS requests. The behavior of these calls has been verified on Solaris Operating System clients and should be the same on other UNIX clients.

`access(2)`

Any check for write permission on a WORM file (that is, a call to `access(2)` where the `amode` argument includes the `W_OK` bit) fails and returns an error (`EPERM`).

`chmod(2)`, `fchmod(2)`

If the target file is a regular, non-WORM file with none of the execute permission bits set, and the new access permission is 4000 (`S_ISUID`), then the target file becomes a WORM file. When this happens, the file receives a new access mode that

is computed by adding the `setuid` bit to any existing read bits in the file's access mode. More specifically, given an old access mode, `oldmode`, a file's new access mode after receiving the WORM trigger can be computed as:

```
newmode = S_ISUID | (oldmode & 0444)
```

Executable files cannot be converted to WORM. Applying the WORM trigger (mode 4000) to a file with one or more execute permission bits fails and returns an error (`EACCES`).

Read access bits can be set or cleared on WORM files. Any attempt to enable write or execute permission on a WORM file, to set the `setgid` bit (`S_ISGID`) or sticky bit (`S_ISVTX`), or to clear the `setuid` bit on a WORM file fails and returns an error (`EPERM`).

`chown(2), fchown(2)`

These calls behave the same on WORM files as on non-WORM files.

`link(2)`

Clients can create new hard links to WORM files. Hard links to a WORM file cannot be removed until the file's retention period ends. (See `unlink(2)`, on page 215).

`read(2), readv(2)`

Clients can read WORM files. Because retention timestamps are stored in the `atime` attribute, this value is not updated to reflect read access to WORM files.

`rename(2)`

Any attempt to rename a WORM file or a non-empty directory on a compliance-enabled file system fails and returns an error (`EPERM`).

`stat(2), fstat(2)`

When these calls are used to obtain information about regular files, the returned `stat` structure contains compliance-related values. The `st_mode` field contains (as always) the file's mode and permissions. A WORM file has the `setuid` bit set and

no write or execute bits. The `st_atime` field contains a timestamp indicating the end of the file's retention period. If this value is equal to `INT_MAX`, as defined in `limits.h`, then the file is retained permanently.

`unlink(2)`

WORM files can only be unlinked if the current time, reflected by the Sun StorEdge 5210 NAS Appliance secure clock, is later than the date stored in the file's `atime` attribute (that is, the retention timestamp). If this condition does not hold, `unlink(2)` fails and returns an error (`EPERM`).

`utime(2), utimes(2)`

These calls are used to set a file's access time (`atime`) and modification time (`mtime`) attributes. When used on a non-WORM file, they behave normally and provide a mechanism for specifying the retention timestamp before a file is converted to WORM.

When invoked on a WORM file, these calls can be used to extend the file's retention period or to assign a new retention period to a file with expired retention. These calls succeed on a WORM file if the new `atime` value is greater than (that is, after) the file's existing `atime` value. If the new `atime` value is less than or equal to the current `atime` value, these calls fail and return an error (`EPERM`). When used on a WORM file, the `mtime` argument is ignored.

`write(2), writev(2)`

Any attempt to write to a WORM file fails and returns an error (`EPERM`).

Behavior of Windows Clients

The following subsections describe differences in compliance-enabled files for Windows clients.

Creating WORM Files

A regular, non-WORM file can only be converted to a WORM file from Windows setting both the read-only and the system bit on a file. The WORM trigger sets the file's read-only bit, but does not change the state of the file's 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.

Metadata Restrictions on WORM Files

Windows clients may change the archive bit on a WORM file. They may not change the read-only, hidden, or system bits. Windows clients can change ACLs on WORM files, but any write permissions in the ACL of a WORM file is ignored. Any attempt to modify the data in a WORM file fails regardless of the permissions in the ACL.

Setting Retention Periods

Like UNIX clients, Windows clients set retention periods by storing retention timestamps in a file's access time (`atime`) attribute.

Caveats for Windows Clients

The following subsections contain additional information you need to be aware of for Windows clients.

Precautions with Read-Only Bit

It is especially important that compliance-enabled file volumes only be used by Windows applications and users that are aware of the special behavior of WORM files. Many standard Windows utilities for copying files will include the read-only and system bits on a file. If these tools are used to make copies of WORM files on a compliance-enabled volume, the resulting files may become WORM files by virtue of having their read-only and system bits set.

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 afterward reset the `atime` to the value it had before the scan. This can lead to a race condition if the virus-checking program scans a file at the same time that another application is setting a retention time on the file. As a result, the file may wind up with the wrong retention time.

A simple way to avoid this problem is to make sure that virus-checking programs do not run on compliance-enabled file systems or do not run at the same time as applications that create WORM files.

Custom applications can also avoid this issue by using a short default retention period and setting a file's true retention period after applying the WORM trigger.

Other APIs

The Compliance Archiving Software can be accessed through many other client APIs, such as Java, Perl, and C++. All of these languages rely on the same underlying system calls to access shares mounted through NFS or CIFS.


Sending a Diagnostic Email Message

The diagnostic email feature enables you to send email messages to the Sun Microsystems Technical Support team or any other desired recipient. Diagnostic email messages include information about the Sun StorEdge 5210 NAS Appliance system configuration, disk subsystem, file system, network configuration, Server Message Block (SMB) shares, backup and restore processes, /etc directory, system log, environment data, and administrator information.

Every diagnostic email message sent includes all of this information, regardless of the problem.

In a cluster configuration, you must set up diagnostic email for each server in the cluster.

To set up diagnostic email:

1. **In the toolbar at the top of the screen, select the  button.**

The Diagnostic Email windows displayed.

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 22.

4. **Click Send to send the message.**

Index

A

access rights, defined 70

accessing
 checkpoints 149

activating, options 101

Active Directory Service
 see ADS

active server
 configuring
 GUI 103
 telnet 183

 mirroring
 defined 103
 telnet 183

activity monitor, viewing, telnet 191

adapters, network
 configuring 13

adapters, network, configuring
 telnet 159

adding
 checkpoints
 GUI 144
 telnet 197
 directory tree quotas 95
 file volume
 telnet 169
 group members
 GUI 72
 telnet 176
 group quotas 93
 hosts
 telnet 181

LUN 31
NFS exports 97
RAID 31
segment
 telnet 170
static shares
 GUI 87
 telnet 173
trusted hosts
 GUI 73
 telnet 181
user quotas 93

administrator
 group 70

ADS
 about 61, 62
 configuring
 GUI 63
 telnet 174
 Windows 2000 clients 91
 container names 64
 defined 8
 enabling 63
 publishing shares 65
 removing shares 66
 setting up 15
 GUI 63
 telnet 174
 updating share containers 66

aggregating
 see bonding ports

alert
 events, system log 124

- mirror buffer thresholds 108
- alias IP address
 - about 58
- anti-virus protection
 - setting up 53
- assigning
 - hot spare 34
 - language 24
 - port roles 14
 - server name 12
- attaching segments
 - telnet 170
- autohome shares
 - about 91
 - configuring 91
 - setting up, telnet 172

B

- backup
 - cleaning the heads 151
 - configuring, telnet 197
 - NDMP
 - GUI 149
 - telnet 198
 - operators group 70
 - viewing
 - job status 139
 - log 139
 - tape status 139
- bonding ports 58
 - viewing, telnet 192
- breaking mirrors
 - GUI 108
 - server 1
 - GUI 111
 - telnet 188
 - telnet 188

C

- CATIA character translations 150
- changing
 - directory tree quotas 96
 - group quotas 94
 - hosts
 - telnet 181
 - language
 - telnet 164

- mirrors 106
 - name services lookup order 67
 - telnet 168
 - NFS exports 99
 - partition names, telnet 170
 - scheduled checkpoint 147
 - static shares
 - GUI 89
 - telnet 174
 - user quotas 94
- channel bonding
 - see bonding ports
- checkpoints
 - about 144
 - accessing 149
 - adding to schedule
 - telnet 197
 - analysis, viewing from telnet 192
 - creating 144
 - editing the schedule 147
 - removing 148
 - removing scheduled 147
 - renaming 147
 - scheduling
 - GUI 145
 - telnet 197
 - sharing 148
- CIFS
 - autohome shares
 - configuring 91
 - setting up, telnet 172
 - Compliance Archiving Software 198
 - configuring clients
 - DOS 91
 - Windows 90
 - defined 85
 - drive letter mapping 168
 - share name limits 87, 89
 - static shares
 - about 85
 - adding 87
 - configuring 86
 - creating 87
 - editing 89
 - removing 90
 - security 88
 - setting up, telnet 171
- clients

- configuring 90
 - DOS 91
 - Windows 90
- cluster
 - port roles 14
- command-line interface 155
- Common Internet File System
 - see CIFS
- Compliance Archiving Software 113
 - API 207
 - configuring 198
- configuring
 - active server
 - GUI 103
 - telnet 183
 - ADS 15
 - GUI 63
 - telnet 174
 - autohome shares
 - GUI 91
 - telnet 172
 - backup
 - telnet 197
 - Compliance Archiving Software 198
 - date 52
 - telnet 160
 - directory tree quotas 95
 - DNS
 - GUI 17
 - telnet 165
 - drive letters in telnet 168
 - dynamic DNS
 - telnet 165
 - email notification 22
 - telnet 190
 - FTP 142, 195
 - gateway address 14
 - group
 - privileges 70
 - privileges, telnet 177
 - quotas 92
 - hosts
 - GUI 73
 - language
 - GUI 24
 - telnet 164
 - LDAP 67
 - local logging
 - telnet 165
 - logging 23
 - mirror server
 - GUI 103
 - telnet 183
 - mirroring
 - telnet 183
 - mirroring file volumes
 - GUI 104
 - telnet 185
 - name services 21
 - telnet 164
 - NDMP
 - GUI 149
 - telnet 198
 - network adapters 13
 - NFS exports 97
 - NICs 13
 - NIS 19
 - NIS+ 20
 - telnet 167
 - NTP 51
 - telnet 161
 - ports
 - GUI 13
 - mirroring 104
 - telnet 159
 - privileges
 - GUI 73
 - telnet 177
 - RDATE 52
 - telnet 161
 - remote logging
 - telnet 165
 - running the wizard 7
 - server name 12
 - SMB/CIFS clients 90
 - SMTP
 - telnet 191
 - SNMP
 - GUI 120
 - telnet 190
 - source server
 - GUI 103
 - telnet 183
 - starting the wizard 8
 - static shares
 - GUI 86
 - telnet 171

- target server
 - GUI 103
 - telnet 183
 - TCP/IP
 - telnet 159
 - time 52
 - telnet 160
 - time synchronization
 - GUI 51
 - telnet 161
 - time zone
 - GUI 52
 - telnet 160
 - user groups, telnet 176
 - user quotas 92
 - variations of the wizard 7
 - verifying DNS for ADS 65
 - warning thresholds 107
 - Windows security 15
 - WINS 17
 - consistency spots, about 144
 - console 155
 - locking 183
 - containers, updating ADS shares 66
 - content panel
 - using 6
 - controller
 - information, viewing 137
 - conventions
 - server names 12
 - creating
 - checkpoints
 - GUI 144
 - telnet 197
 - directory tree quotas 95
 - file volume 34
 - telnet 169
 - group quotas 93
 - hosts
 - telnet 181
 - LUN 31
 - NFS exports 97
 - RAID 31
 - scheduled checkpoint
 - telnet 197
 - segment 34
 - telnet 170
 - static shares
 - GUI 87
 - telnet 173
 - trusted hosts
 - GUI 73
 - telnet 181
 - user quotas 93
 - creating a file system 30
 - credentials, mapping 75
 - critical events, system log 124
 - c-spots, about 144
- ## D
- date, setting 52
 - telnet 160
 - debug events, system log 124
 - dedicated port
 - mirroring 104
 - setting port role 104
 - default quotas
 - group 92
 - user 92
 - defining
 - file volume 34
 - LUN 31
 - RAID 31
 - segment 34
 - deleting
 - checkpoint 148
 - directory tree quotas 97
 - group members
 - GUI 72
 - telnet 177
 - hosts
 - GUI 74
 - telnet 181
 - mirrored file volume
 - telnet 189
 - NFS exports 99
 - out-of-date file volume
 - GUI 111
 - telnet 189
 - quarantined files 56
 - scheduled checkpoint 147
 - static shares
 - GUI 90
 - telnet 174
 - trusted hosts

- GUI 74
- telnet 182
- user quotas 95
- diagnostic email, sending 219
- directory tree quotas
 - adding 95
 - configuring 95
 - deleting 97
 - editing 96
- displaying
 - routes 134
 - system events 124
 - system log 122
- DN, defined 16
- DNS
 - about 62
 - setting up
 - GUI 17
 - telnet 165
 - verifying configuration 65
- domain
 - security 15
- DOS, configuring for SMB/CIFS 91
- drive letters, configuring, telnet 168
- DTQ
 - defined 95
 - see directory tree quota
- dual server systems
 - port roles 14
- dynamic DNS
 - enabling 18
 - setting up, telnet 165

E

- editing
 - directory tree quotas 96
 - group quotas 94
 - hosts
 - telnet 181
 - keys used in telnet 157
 - mirrors 106
 - NFS exports 99
 - scheduled checkpoint 147
 - static shares
 - GUI 89
 - telnet 174
 - user quotas 94

- email notification
 - configuring, telnet 190
 - diagnostic, sending 219
 - notification levels 23
 - setting up 22
- emergency events, system log 124
- enabling
 - ADS
 - GUI 63
 - telnet 174
 - anti-virus protection 53
 - autohome shares
 - GUI 92
 - telnet 172
 - checkpoints
 - telnet 197
 - DNS
 - GUI 17
 - telnet 165
 - domain security 15
 - dynamic DNS 18
 - telnet 165
 - email notification 22
 - telnet 190
 - foreign languages
 - GUI 24
 - telnet 164
 - group quotas
 - GUI 93
 - telnet 175
 - LDAP 67
 - logging 23
 - name services 21
 - telnet 164
 - NIS 19
 - NIS+ 20
 - telnet 167
 - quotas
 - telnet 175
 - remote logging
 - telnet 165
 - SNMP
 - GUI 120
 - telnet 190
 - static shares
 - GUI 87
 - telnet 171
 - UPS monitoring 136
 - user quotas

- GUI 93
 - telnet 175
- WINS 17
- workgroup security 15
- environmental status
 - system fans 127
 - system power supplies 129
 - temperature 128
 - viewing 127
 - voltage 130
- error events, system log 124
- error messages 201
 - file system errors 204
 - IPMI events 205
 - RAID subsystem errors 204
 - SysMon 201
 - UPS subsystem errors 202
- events
 - IPMI 205
 - logging in telnet 166
 - system log 124
- exports
 - creating 97
 - editing 99
 - removing 99
 - setting up 97

F

- facility
 - telnet 165
- fan
 - status 127
- file directory security 82
- File Replicator 103
- file system
 - creating 30
 - error messages 204
 - managing in telnet 168
- file system errors 204
- File Transfer Protocol
 - see FTP
- file volume
 - about 30
 - autohome shares
 - about 91
 - telnet 172
 - creating 34

- telnet 169
- deleting out-of-date volume
 - GUI 111
 - telnet 189
- expanding
 - telnet 170
- managing access, telnet 182
- mirroring
 - GUI 104
 - telnet 185
- mirroring up-to-date volume
 - GUI 111
 - telnet 189
- name limits 35
- promoting
 - GUI 109
 - telnet 187
- re-establishing mirror
 - GUI 110
 - telnet 188
- static shares
 - about 85
 - telnet 171
- usage statistics 131

FTP

- access 143, 195
- configuring 142, 195

G

- gateway address
 - setting 14
- GID, defined 88
- graphical user interface
 - see GUI
- group
 - adding members
 - GUI 72
 - telnet 176
 - administrators 70
 - backup operators 70
 - credentials, mapping 75
 - power users 70
 - privileges
 - GUI 70
 - telnet 177
 - quotas
 - adding 93
 - configuring 92

- default 92
 - editing 94
 - removing members
 - GUI 72
 - telnet 177
 - root
 - quotas 93
 - user, about 69
- GUI
 - content panel 6
 - defined 1
 - navigation panel 3
 - online help 7
 - Status panel 6
 - toolbar 2
- H**
- hard limits 92
- head
 - cleaning 151
- help, using 7
- hosts
 - adding
 - telnet 181
 - configuring 73
 - deleting, telnet 181
 - editing
 - telnet 181
 - naming 74
 - removing 74
 - routes 134
 - trusted 73
 - adding, telnet 181
 - configuring 73
 - deleting, telnet 182
 - removing 74
 - telnet 181
- hot spare
 - assigning 34
- I**
- icons, toolbar 2
- identifying port locations 13, 57
- immediate
 - checkpoints, creating 144
- independent, port role 57
- individual mirrors, viewing status from telnet 192
- information events, system log 124
- IP address
 - aliasing 58
- IP aliases
 - about 58
- IPMI events 205
- iSCSI configuration 43
- iSNS server 48
- K**
- KDC, defined 16
- key distribution center
 - see KDC
- L**
- language
 - assigning 24
 - selecting, telnet 164
- LDAP
 - about 61
 - configuring 67
 - enabling 67
 - setting up 67
- Lightweight Directory Access Protocol
 - see LDAP
- limits
 - hard 92
 - names
 - ADS container 64
 - container 64
 - domain 15
 - file volume 35
 - host 74
 - NetBIOS 15
 - scope 17
 - segment 35
 - server 12
 - share 87, 89
 - soft 92
- local logging
 - see logging
- locking the console 183
- logging
 - alert events 124
 - backup log
 - GUI 139
 - critical events 124

- debug events 124
- displaying the log 122
- emergency events 124
- error events 124
- event types 166
- facilities 23
 - telnet 165
- information events 124
- local, setting up
 - telnet 165
- notice events 124
- remote, setting up
 - telnet 165
- setting up 23
- system events 124
- viewing system log
 - GUI 122
 - telnet 192
- warning events 124

lookup order

- changing 67
- name services, verifying 64
- setting in telnet 168

LUN

- about 29
- adding 31
- creating 31
- defined 29
- rebuilding 38

M

Macintosh

- desktop DB calls 87, 89
- support 87, 89

main menu, telnet 158

managing

- file volume access, telnet 182
- quotas 92
- routes, telnet 164
- trusted hosts, telnet 181

mapping

- credentials 75
- drive letters, telnet 168

messages

- display language 24

MIB files 120

mirror

buffer

- defined 103
- threshold alerts 108

port role 57

server

- configuring 103
- configuring, telnet 183
- defined 103
- setting up 103

mirroring

- about 103
- active server, defined 103
- before you begin 103
- breaking
 - mirror 108
 - telnet 188
- changing 106
- configuring
 - active server, telnet 183
 - dedicated port 104
 - file volumes, telnet 185
 - mirror server, telnet 183
 - source server, telnet 183
 - target server, telnet 183
- deleting file volume, telnet 189

editing 106

mirror buffer, defined 103

mirror server, defined 103

promoting file volume

- GUI 109
- telnet 187

re-establishing a mirror

- GUI 110
- telnet 188

requirements 103

setting up

- dedicated port 104
- file volumes 104
- telnet 185

setting warning thresholds, telnet 186

source server, defined 103

status states 138

target server, defined 103

telnet 183

usage statistics 137

viewing, telnet

- individual status 192
- statistics 194

modifying, telnet

- group privileges 177
- monitoring
 - configuring SNMP 120
 - UPS 135
 - enabling 136

N

- name
 - container, limits 64
 - domain 15
 - file volume 35
 - hosts 74
 - NetBIOS limitation 15
 - scope 17
 - segment 35
 - server
 - conventions 12
 - share name limits 87, 89
- name services
 - changing lookup order 67
 - configuring 21
 - DNS 21
 - local 21
 - NIS 21
 - NIS+ 21
 - setting lookup order, telnet 168
 - verifying lookup order 64
- name, server
 - setting 12
- navigating
 - telnet 157
 - Web Administrator 1
- navigation panel
 - using 3
- NDMP
 - defined 149
 - setting up 149
 - setting up in telnet 198
- network
 - activity, usage statistics 131
 - routes 134
 - displaying 134
 - statistics 134
- Network Data Management Protocol
 - see NDMP
- Network File System
 - see NFS

- Network Information Service
 - see NIS
 - Network Information Service Plus
 - see NIS+
 - Network Time Protocol
 - see NTP
 - NFS
 - defined 97
 - exports
 - creating 97
 - editing 99
 - removing 99
 - setting up 97
 - NIC
 - configuring 13
 - NIS
 - about 62
 - defined 8
 - setting up 19
 - NIS+
 - about 62
 - defined 8
 - setting up 20
 - telnet 167
 - notice events, system log 124
 - notification levels, email notification 23
 - NSSLDAP, see LDAP
 - NTP
 - defined 50
 - setting up 51
 - telnet 161
 - time synchronization 50
 - telnet 161
- ## O
- online help, using 7
 - options
 - activating 101
 - Compliance Archiving Software 113, 198
 - API 207
 - mirroring 103
 - ownership assignment, group privilege 71
- ## P
- parity, defined 28
 - partition
 - about 29

- renaming, telnet 170
- password
 - administrator, setting 49
- path names, ADS 64
- ports
 - bonding 58
 - configuring
 - telnet 159
 - location
 - identifying 13, 57
 - mirroring
 - configuring 104
 - setting up 104
 - roles 58
 - assigning 14
 - independent 57
 - mirror 57
 - primary 57
 - setting dedicated port 104
 - viewing port bonds, telnet 192
- power supply
 - status 129
- power users group 70
- primary, port role 57
- privileges
 - configuring 73
 - defined 70
 - ownership assignment 71
 - root user 73
 - user groups 70
- promoting
 - file volume
 - GUI 109
 - telnet 187
- publishing shares in ADS 65

Q

- quarantined files
 - deleting 56
- quotas
 - default group 92
 - default user 92
 - directory tree
 - adding 95
 - configuring 95
 - deleting 97
 - editing 96

- enabling
 - telnet 175
- group
 - adding 93
 - configuring 92
 - editing 94
- hard limits 92
- managing 92
- root group 93
- root user 93
- soft limits 92
- user
 - adding 93
 - configuring 92
 - deleting 95
 - editing 94

R

RAID

- about 27
- adding 31
- creating 31
- error messages 204
- levels supported 27
- parity, defined 28
- sets 27
- striping, defined 28
- RAID subsystem errors 204

RDATE

- setting up 52
 - telnet 161
- time synchronization 50
 - telnet 161

rebooting

- server 144
- telnet 196

rebuilding, LUN 38

- Redundant Array of Independent Disks
 - see RAID

re-establishing a mirror

- breaking the mirror
 - GUI 111
 - telnet 188
- deleting out-of-date file volume
 - GUI 111
 - telnet 189
- GUI 110
- mirroring up-to-date file volume

- GUI 111
- telnet 189
- telnet 188
- remote logging
 - see logging
 - setting up
 - telnet 165
- removing
 - checkpoint 148
 - directory tree quotas 97
 - group members
 - GUI 72
 - telnet 177
 - hosts
 - GUI 74
 - telnet 181
 - NFS exports 99
 - scheduled checkpoint 147
 - shares from ADS 66
 - static shares
 - GUI 90
 - telnet 174
 - trusted hosts
 - GUI 74
 - telnet 182
- renaming
 - checkpoint 147
 - partitions, telnet 170
- requirements
 - mirroring 103
 - server name 12
- restore
 - cleaning the heads 151
- retention period, Compliance Archiving Software 198
- root group
 - quotas 93
- root user
 - privileges defined by host status 73
 - quotas 93
- routes
 - about 134
 - displaying 134
 - flags 134
 - host 134
 - managing in telnet 164
- running

- configuration wizard 7
- head cleaning 151

S

- scheduling
 - checkpoints 145
 - editing 147
 - removing 147
 - telnet 197
- security
 - administrator password 49
 - file volume access, telnet 182
 - locking the console 183
 - setting 83
 - static shares 88
 - unlocking the console 183
 - Windows 15
- segment
 - about 30
 - adding, telnet 170
 - attaching
 - telnet 170
 - creating 34
 - name limits 35
- selecting language, telnet 164
- sending a diagnostic email 219
- server
 - name
 - conventions 12
 - setting 12
 - reboot 144
- Server Message Block
 - see SMB
- setting
 - administrator password 49
 - date 52
 - telnet 160
 - gateway address 14
 - group quotas 92
 - language
 - telnet 164
 - name services lookup order 21
 - telnet 168
 - security 83
 - server name 12
 - time 52
 - telnet 160
 - time zone 52

- telnet 160
- user quotas 92
- warning thresholds
 - GUI 107
 - telnet 186
- setting up
 - active server
 - GUI 103
 - telnet 183
 - ADS 15
 - GUI 63
 - telnet 174
 - autohome shares
 - GUI 91
 - telnet 172
 - backup, telnet 197
 - Compliance Archiving Software 198
 - directory tree quotas 95
 - DNS
 - GUI 17
 - telnet 165
 - drive letters, telnet 168
 - dynamic DNS
 - telnet 165
 - email notification 22
 - telnet 190
 - FTP 142, 195
 - group privileges 70
 - hosts 73
 - language 24
 - LDAP 67
 - local logging
 - telnet 165
 - mirror server
 - GUI 103
 - telnet 183
 - mirroring
 - telnet 185
 - mirroring file volumes 104
 - name services 21
 - NDMP
 - GUI 149
 - telnet 198
 - network adapters 13
 - NFS exports 97
 - NICs 13
 - NIS 19
 - NIS+ 20
 - telnet 167

- NTP 51
 - telnet 161
- ports
 - GUI 13
 - mirroring 104
 - telnet 159
- privileges 73
- RDATE 52
 - telnet 161
- remote logging
 - telnet 165
- SMB/CIFS clients 90
- SNMP
 - GUI 120
 - telnet 190
- source server
 - GUI 103
 - telnet 183
- static shares
 - GUI 86
 - telnet 171
- target server
 - GUI 103
 - telnet 183
- TCP/IP, telnet 159
- time synchronization 51
 - telnet 161
- Windows security 15
- WINS 17
- shares
 - about 85
 - autohome
 - about 91
 - configuring 91
 - setting up, telnet 172
 - checkpoints 148
 - mapping drive letters 168
 - naming limits 87, 89
 - publishing in ADS 65
 - removing from ADS 66
 - static
 - about 85
 - adding, telnet 173
 - configuring 86
 - creating 87
 - deleting, telnet 174
 - editing 89
 - editing, telnet 174
 - removing 90

- security 88
 - setting up, telnet 171
 - updating ADS containers 66
- shut down
 - telnet 196
- shutting down 143
- Simple Mail Transfer Protocol
 - see SMTP
- Simple Network Management Protocol
 - see SNMP
- SMB
 - autohome shares
 - configuring 91
 - enabling 92
 - configuring
 - clients 90
 - DOS clients 91
 - Windows clients 90
 - defined 85
 - drive letter mapping 168
 - security, static shares 88
 - setting up
 - autohome shares, telnet 172
 - static shares, telnet 171
 - share name limits 87, 89
 - static shares
 - about 85
 - adding 87
 - changing 89
 - configuring 86
 - creating 87
 - deleting 90
 - editing 89
 - enabling 87
 - removing 90
- SMTP
 - defined 22
- SNMP
 - configuring
 - GUI 120
 - telnet 190
 - defined 120
- soft limits 92
- software
 - File Replicator 103
 - mirroring 103
 - updating 152
- source server
 - configuring
 - GUI 103
 - telnet 183
 - mirroring
 - defined 103
 - telnet 183
- static shares
 - about 85
 - configuring 86
 - creating 87
 - editing 89
 - name limits 87, 89
 - removing 90
 - security 88
- status 121
 - backup jobs 139
 - backup tapes 139
 - controller information 137
 - environmental, viewing 127
 - fans 127
 - file volume usage 131
 - individual mirrors, telnet 192
 - mirror states 138
 - mirror statistics, telnet 194
 - mirroring
 - GUI 137
 - telnet 192
 - network activity 131
 - network routes 134
 - power supplies 129
 - system activity 132
 - temperature 128
 - UPS 135
 - voltage 130
- striping, defined 28
- Sun StorEdge File Checkpoints
 - see checkpoints
- supported RAID levels 27
- Synchronizing time
 - setting up 51
- synchronizing time
 - about 50
 - telnet 161
- syslogd, defined 23
- SysMon, about 201
- system

- activity usage statistics 132
- events
 - displaying 124
- log
 - displaying 122
 - viewing, telnet 192
- shutting down
 - GUI 143
 - telnet 196
- status
 - panel, using 6

T

- target server
 - configuring
 - GUI 103
 - telnet 183
 - defined 103
 - mirroring, telnet 183
- TCP/IP
 - configuring
 - telnet 159
- telnet
 - adding
 - checkpoints 197
 - group members 176
 - hosts 181
 - segments 170
 - shares 173
 - trusted hosts 181
 - breaking mirrors 188
 - configuring
 - active server 183
 - backup 197
 - drive letters 168
 - email notification 190
 - mirror server 183
 - mirrored file volumes 185
 - SNMP 190
 - source server 183
 - target server 183
 - TCP/IP 159
 - user groups 176
 - creating file volumes 169
 - deleting
 - hosts 181
 - mirrored file volume 189
 - shares 174
 - trusted hosts 182
 - edit keys 157
 - editing
 - hosts 181
 - shares 174
 - enabling quotas 175
 - locking console 183
 - logging
 - events 166
 - facilities 165
 - main menu 158
 - managing
 - file system 168
 - file volume access 182
 - routes 164
 - trusted hosts 181
 - menus 157
 - mirroring 183
 - breaking mirrors 188
 - promoting file volumes 187
 - viewing status 192
 - modifying
 - group privileges 177
 - navigating 157
 - rebooting 196
 - re-establishing mirrors 188
 - removing group members 177
 - renaming partitions 170
 - scheduling
 - checkpoints 197
 - selecting, language 164
 - setting
 - date 160
 - name services lookup order 168
 - time 160
 - time synchronization 161
 - time zone 160
 - warning thresholds 186
 - setting up
 - ADS 174
 - autohome shares 172
 - DNS 165
 - dynamic DNS 165
 - local logging 165
 - mirrors 185
 - NDMP 198
 - NIS+ 167
 - NTP 161
 - RDATE 161

- remote logging 165
- static shares 171
- shutting down 196
- unlocking console 183
- viewing
 - activity monitor 191
 - checkpoint analysis 192
 - individual mirror status 192
 - mirror statistics 194
 - mirror status 192
 - port bonding 192
 - system log 192
- temperature status 128
- thresholds, setting
 - GUI 107
 - telnet 186
- time
 - setting 52
 - telnet 160
 - synchronization
 - about 50
 - NTP 50
 - RDATE 50
 - setting up 51
 - setting, telnet 161
 - zone, setting 52
 - telnet 160
- toolbar
 - icons 2
 - using 2
- trunking
 - see bonding ports
- trusted hosts
 - about 73
 - adding
 - GUI 73
 - telnet 181
 - deleting, telnet 182
 - managing, telnet 181
 - removing 74
- turning the server off 143
 - telnet 196

U

- UID, defined 88
- umask 88
- Uninterruptible Power Supply

- see UPS
- UNIX settings
 - mapping 80, 81
 - name service lookup order 21
- unlocking console 183
- updating
 - ADS share containers 66
 - software 152
- UPS
 - defined 135
 - enabling monitoring 136
 - error messages 202
 - monitoring 135
- UPS subsystem errors 202
- usage statistics
 - file volumes 131
 - mirroring 137
 - network activity 131
 - system activity 132
- user
 - credentials
 - mapping 75
 - groups
 - about 69
 - adding members, telnet 176
 - configuring, telnet 176
 - modifying privileges, telnet 177
 - privileges 70
 - removing members, telnet 177
 - quotas
 - adding 93
 - configuring 92
 - default 92
 - deleting 95
 - editing 94
 - root
 - quotas 93
- using
 - content panel 6
 - navigation panel 3
 - online help 7
 - Status panel 6
 - toolbar 2

V

- variations, configuration wizard 7
- verify

- DNS configuration 65
- name service lookup order 64
- viewing
 - activity monitor, telnet 191
 - backup
 - job status 139
 - tape status 139
 - backup, log
 - GUI 139
 - checkpoint analysis, telnet 192
 - controller information 137
 - environmental status 127
 - fan status 127
 - file volume usage 131
 - individual mirror status, telnet 192
 - mirror statistics
 - GUI 137
 - telnet 194
 - mirror status, telnet 192
 - network activity 131
 - network routes 134
 - port bonds, telnet 192
 - power supply status 129
 - status 121
 - system activity 132
 - system log
 - GUI 122
 - telnet 192
 - temperature status 128
 - voltage status 130
- virus scanning 55
- voltage status 130

W

- warning events, system log 124
- warning thresholds
 - about 107
 - setting
 - GUI 107
 - telnet 186
- Web Administrator
 - content panel 6
 - navigating in 1
 - navigation panel 3
 - online help 7
 - Status panel 6
 - toolbar 2

Windows

- autohome shares, about 91
- configuring SMB/CIFS 90
- domain
 - enabling 15
- mapping credentials 80
- security
 - models 15
- static shares, about 85
- workgroup
 - enabling 15
 - file directory security 82
 - security 88
- WINS
 - about 62
 - setting up 17
- wizard
 - running 7
 - starting 8
 - variations 7
- workgroup
 - security
 - enabling 15
- WORM files 208