



Sun StorageTek™ NAS OS Administration Guide

NAS Software Version 4.21

Sun Microsystems, Inc.
www.sun.com

Part No. 819-4284-11
March 2007, Revision A

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

Copyright 2007 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, Sun StorageTek, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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, États-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, Sun StorageTek, Java, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

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

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 xxxv

1. Product Overview 1

Introduction 1

Using Web Administrator 1

Logging In 2

Steps to Log In 2

Considerations With Multiple Users 2

About the Interface Layout 4

About the Toolbar 4

About the Navigation Panel 6

About the Folder Symbol Key 7

About Other Buttons 7

About the Content Panel 8

About the Status Panel 9

Using Help 10

Using the Configuration Wizard 11

About Configuration Wizard Variations 11

Running the Wizard 11

Where to Go From Here	13
2. Initial Network Configuration	15
About the Initial Network Configuration	16
Setting the Server Name	16
Managing LUN Paths	17
About Setting LUN Paths	17
About LUN Paths in Single-Server Systems	18
About LUN Paths in Dual-Server Systems	19
Setting LUN Paths	20
Restoring a LUN Path	21
Enabling Failover	21
About Enabling Failover	21
Enabling Server Failover	22
Initiating Failback (Recovery)	23
About Initiating Recovery	24
Initiating Recovery	24
Configuring Network Ports and Adapters	24
About Configuring Network Ports	25
About Network Port Locations	25
Configuring Network Adapters	25
Setting the Default Gateway Address	27
Managing Name Services	27
Configuring Windows Security	28
Setting Up WINS	29
Setting Up DNS	30
Setting Up NIS	31
Setting Up NIS+	32
Configuring Name Services	34

Setting Up Email Notifications	34
Setting Up Logging	35
Assigning the Language	36
Registering the System	36
Backing Up Configuration Information	37
Where to Go From Here	37
3. File-System Setup and Management	39
File-System Concepts	39
About RAID Configurations	40
About RAID Systems	40
About the RAID-0 Configuration (Not Supported)	40
About the RAID-1 Configuration (Gateway Systems Only)	41
About the RAID-1+0 Configuration (Gateway Systems Only)	41
About the RAID-5 Configuration	41
NAS RAID-5 Systems – Sun StorageTek 5310 and Sun StorageTek 5320 Appliances	42
NAS RAID-5 Systems – Sun StorageTek 5210 Appliances	43
About LUNs	43
About Partitions	44
About File Volumes	45
About Segments	45
Creating the File System	46
About Creating the File System	46
About Creating RAID Sets and LUNs	46
Adding a New LUN (Sun StorageTek 5310 and Sun StorageTek 5320 NAS Devices)	48
Adding a New LUN (Sun StorageTek 5210 NAS Appliances)	49
Designating a Drive As a Hot-Spare	49

Creating File Volumes or Segments	50
About Creating a File Volume or a Segment	50
Creating a File Volume or Segment Using the Create File Volumes Panel	51
Creating a File Volume or Segment Using the System Manager	52
Attaching Segments to a Primary File Volume	53
About Attaching Segments to a Primary File Volume	54
Attaching a Segment Using the Attach Segments Panel	54
Attaching a Segment Using the System Manager	54
About Rebuilding a LUN	55
Managing File Volumes and Segments	55
Editing File Volume Properties	56
Deleting File Volumes or Segments	58
Viewing Volume Partitions	58
System Language Considerations	59
Configuring the NAS for iSCSI	59
About iSCSI	60
About iSCSI Identifiers	61
About Configuring an iSCSI Target	62
Creating an iSCSI Access List	62
Creating an iSCSI LUN	63
About SCSI Thin-Provisioned LUNs	63
About iSCSI Target Discovery Methods	64
Specifying an iSNS Server	65
Where to Go From Here	65
4. System Management	67
Setting the Administrator Password	67
Controlling the Time and Date	68
About Controlling the Time and Date	68

About Time Synchronization	68
Setting Up Time Synchronization	69
Setting the Time and Date Manually	70
Using Antivirus Software	70
About Virus Scanning	71
Enabling Antivirus Protection	72
Excluding Files From Scans	72
Enabling Trend Micro Antivirus Protection	73
5. Server Port Management	77
About Port Locations and Roles	77
About Alias IP Addresses	78
Bonding Ports	79
About Port Bonding	79
About Port Aggregation Bonds	79
About High-Availability Bonds	80
Bonding Ports on a Single-Server System	80
Bonding Ports for Cluster Configurations	81
Example: Dual-Server Port Bonding	83
6. Active Directory Service and Authentication	85
About Supported Name Services	85
Using Active Directory Service	86
About Active Directory Service	86
Enabling ADS	87
Verifying Name Service Lookup Order	89
Verifying DNS Configuration	89
Publishing Shares in ADS	90
Updating ADS Share Containers	90

Removing Shares From ADS	91
Setting Up LDAP	91
Changing the Name Service Lookup Order	92
7. Group, Host, and File Directory Security	93
Managing Local Group Privileges	93
About Local Groups	94
About Configuring Privileges for Local Groups	94
About Ownership Assignment and Groups	95
Adding and Removing Group Members and Configuring Privileges	96
Configuring NT Privileges for Groups	97
Configuring Hosts	97
About Configuring Hosts	98
Adding and Editing Hosts	98
About Trusted Hosts	98
Adding a Host Manually	98
Editing Host Information	99
Removing a Host Mapping for a Host	99
Adding and Editing Host Groups	100
About Adding and Editing Host Groups	100
Adding a Host Group	100
Adding a Member to a Host Group	101
Mapping User and Group Credentials	101
About Mapping User and Group Credentials	102
About Unix Users and Groups	102
About Windows Users and Groups	103
About Credential Mapping	104
About User Mapping Policies	105
About User Mapping	105

About User Mapping Policy Settings	105
Example: User Mapping Policy	106
About Group Mapping Policies	106
About Group Mapping	106
About Group Mapping Policy Settings	107
Example: Group Mapping Policy	107
About Built-In Credential Mapping Policies	108
About Built-In Credential Mapping	108
Defining the Mapping Policy	108
Mapping Windows Groups and Users to Unix Groups and Users	109
Editing a Mapping Between a Windows Group or User and a Unix Group or User	110
Setting File Directory Security	111
About Setting File Directory Security in Workgroup Mode	111
Setting File Directory Security in Domain Mode	111
8. Shares, Quotas, and Exports	113
Managing Shares	113
About Shares	114
About Static Shares	114
About Share Access Permissions	115
Configuring Static Shares	116
About Configuring Static Shares	116
Creating Static Shares	116
Editing an Existing SMB Share	118
Removing an SMB/CIFS Share	118
About Configuring SMB/CIFS Clients	119
About Autohome Shares	119
Enabling Autohome Shares	120

Managing Quotas	121
About Managing Quotas	122
Configuring User and Group Quotas	122
About Configuring User and Group Quotas	122
Enabling Quotas for a File Volume	123
Adding a User or Group Quota	123
Editing a User or Group Quota	124
Deleting a User or Group Quota	124
Configuring Directory Tree Quotas	125
About Configuring Directory Tree Quotas	125
Creating a Directory Tree With a Directory Tree Quota	125
Editing an Existing Directory Tree Quota	126
Deleting a Directory Tree Quota	127
Setting Up NFS Exports	127
About Setting Up NFS Exports	128
Creating Exports	128
Editing Exports	129
Removing Exports	130
9. System Options	131
Activating System Options	131
About the Sun StorageTek File Replicator Option	132
About Mirroring	133
About Preparing for Mirroring	134
About Requirements and Limitations for Cluster Configurations	134
Configuring Active and Mirror Servers	135
Configuring Mirrored File Volumes	136
About Mirroring the Mirror Buffer	136
Activating File Replicator Software on the Remote Server	137

Adding a File Volume Mirror	137
Editing a Mirror	138
Avoiding and Correcting a Cracked Mirror	139
Setting Warning Thresholds for Mirrored File Volumes	139
About Setting Warning Thresholds	140
Setting Up the Threshold Alert	140
Breaking the Connection and Promoting a Mirrored File Volume	141
Breaking the Connection Between Mirror Servers	141
Promoting a Mirrored File Volume	142
Promoting iSCSI LUNs	143
Reestablishing Mirror Connections	144
Reestablishing a Mirror Connection	144
Breaking the Mirror Connection on the Active Server	145
Deleting the Out-of-Date File Volume From Server 1	145
Mirroring the Up-to-Date File Volume From Server 2 to Server 1	145
Changing Volume Roles	146
About the Compliance Archiving Option	147
About Compliance Archiving Software	147
About Enabling Compliance Archiving	148
About Compliance With Mandatory Enforcement	148
About Compliance With Advisory Enforcement	149
About Compliance Auditing	149
About the Assured Delete Option	151
About Assured Delete	152
Enabling Assured Delete	152
About Restrictions for Assured Delete	153

10. Monitoring the System	155
SNMP Monitoring	155
About SNMP Monitoring	156
Setting Up SNMP	156
Viewing System Status	157
System Logging	157
About System Logging	158
About System Events	159
Viewing the System Log	160
System Auditing	160
About System Auditing	161
About Audit Log Files	161
Setting Up System Auditing	162
Viewing Environmental Status	162
Viewing Fan Status	163
Viewing Temperature Status	163
Viewing Power Supply Status	163
Viewing Voltage Status	164
Viewing Usage Information	165
Viewing File Volume Usage	165
Viewing Network Activity	165
Viewing System Activity	165
Viewing Network (Port) Statistics	166
Viewing Network Routes	166
About Network Routes	166
Displaying Routes	167
Monitoring System Status	167
About UPS Monitoring	168

Enabling UPS Monitoring	168
Viewing Controller Information	169
Viewing the Mirror Status	169
Viewing Mirroring Statistics	169

11. System Maintenance 171

Setting Remote Access Options	171
Configuring FTP Access	172
About Configuring FTP Access	172
Setting Up FTP Users	173
Shutting Down the Server	174
Locating a Drive or Controller/Expansion Unit	174
Configuring the LAN Manager Compatibility Level	175
Managing File-System Checkpoints	176
About File-System Checkpoints	176
Enabling File-System Checkpoints	177
Scheduling File-System Checkpoints	178
About Scheduling File-System Checkpoints	178
Adding a Checkpoint to the Schedule	179
Editing an Existing Checkpoint Schedule	179
Removing a Schedule Line	180
Creating a Manual Checkpoint	180
Renaming a Checkpoint	181
Removing a Checkpoint	181
Sharing File-System Checkpoints	182
Accessing Checkpoints	183
Managing RAID Controllers	184
Controlling LEDs	184
Getting Events and Configuration Information	184

Setting the Controller Time and Battery Age	185
Downloading RAID Array and Drive Firmware	186
Mounting File Systems	186
Setting Up NDMP Backups	186
Updating the Time Zone Database	188
Enabling CATIA V4/V5 Character Translations	189
About CATIA V4/V5 Character Translations	189
Enabling CATIA Manually	190
Enabling CATIA Automatically	190
Backing Up Configuration Information	191
Upgrading NAS Software	191
Upgrading Software With a Reboot	192
Upgrading Cluster Software Without Interrupting Service	192
Configuring the Compliance Archiving Software	194
Changing the Default Retention Period	194
Enabling CIFS Compliance	195
Upgrading Array and Drive Firmware Revision Levels	195
Determining If You Need to Upgrade the Firmware	196
Upgrading Array and Drive Firmware (Reboot Required)	196
Upgrading Array Firmware (No Reboot Required)	199
Upgrading Drive Firmware (Reboot Required)	204
Capturing <code>raidctl</code> Command Output	205
Capturing <code>raidctl</code> Command Output From a Solaris Client	205
Capturing <code>raidctl</code> Output From a Windows Client	216

12. Replacing Components	217
Tools and Supplies Needed	217
Powering Off	218
Removing the Covers	220
Removing the Main Cover	220
Removing the Front Bezel	221
Removing the Front Cover	223
Locations of Customer-Replaceable Units	224
Replacing Components	224
Replacing a Fan Connector Board	225
Replacing the Front Panel Indicator Board	227
Replacing the Power Supply	229
Replacing Memory Modules	231
Replacing a Fan Module Assembly	233
Replacing the Rear Fan Tray	235
Replacing a PCI Card	236
A. Console Administration	241
Accessing the Administrator Console	242
Opening a telnet Session	242
Console Menu Basics	243
Viewing Man Pages	244
System Management	244
Configuring TCP/IP	244
Modifying the Administrator Password	245
Setting the Time and Date	245
Setting Time Synchronization	246
Enabling Antivirus Protection	248
Selecting a Language	249

Managing Routes	249
Name Services	250
Setting Up DNS, Remote Log, and Local Log	250
Setting Up a Name Service	251
Setting Lookup Order for Name Service	252
Managing the Server File System	253
Configuring Drive Letters	253
Creating a New Disk Volume	254
Renaming a Partition	254
Adding an Extension Segment	255
Deleting a Disk Volume	255
Shares and Quotas	256
SMB/CIFS Shares	256
Setting Up SMB/CIFS Shares	256
Setting up SMB/CIFS Autohome Shares	257
Adding a Share	258
Editing a Share	259
Deleting a Share	260
Setting Up Active Directory Service	260
Enabling and Disabling Quotas	261
Security	261
Configuring User Groups	262
Adding a Group	262
Adding a Member to a Group	262
Removing a Member From a Group	263
Modifying Group Privileges	263
User and Group Maps	264
Adding a User Map	264

Editing a User Map	264
Removing a User Map	265
Adding a Group Map	265
Editing a Group Map	265
Removing a Group Map	266
Mapping and Securable Objects	266
Using the chsmb Command	267
Using the acl.override.allowed Environment Variable	267
Configuring the Host List	268
Adding a Host	268
Editing an Existing Host	268
Deleting a Host	268
Managing Trusted Hosts	269
Adding a Trusted Host	269
Deleting a Trusted Host	269
Managing Volume Access for NFS Clients	270
Locking and Unlocking the Console	270
Locking the Console	271
Unlocking the Console	271
Mirroring File Volumes	271
Configuring Active and Mirror Servers	272
Configuring a New Active Server With a New Mirror Server	272
Configuring an Existing Active Server With a New Mirror Server	273
Configuring File Volumes	273
Setting Up a File Volume for Mirroring	274
Mirroring File Volumes	274
Setting Warning Thresholds	275
Breaking the Connection and Promoting a Mirrored File Volume	276

Breaking the Connection Between Mirror Servers	276
Promoting a Mirrored File Volume	277
Promoting iSCSI LUNs	278
Reestablishing a Mirror	278
Breaking the Mirror on Server 1	279
Deleting the Out-of-Date File Volume on Server 1	279
Mirroring the Up-to-Date File Volume on Server 2 Back to Server 1	280
Changing Roles	280
Monitoring	281
Configuring SNMP	281
Configuring Email Notification	281
Configuring Diagnostic Logs	282
Viewing System Information	284
Viewing Server Status	284
Viewing the System Log	285
Viewing Port Bonding	285
Viewing the Checkpoint Analysis	285
Viewing the Status of a Mirrored File Volume	285
Viewing Network Statistics for All Mirrored File Volumes	287
Configuring the NAS for iSCSI	288
Creating an iSCSI Access List	289
Creating an iSCSI LUN	290
Specifying an iSNS Server	291
System Maintenance	292
Configuring File Transfer Protocol (FTP) Access	292
Types of Users	292
Setting Up FTP Access	293
Shutting Down the System	293

Managing Head Failover	294
Configuring Failover	294
Restoring the System, Initiating Failback	295
Configuring LUN Paths	295
Scheduling File Checkpoints	296
Configuring NDMP Backup	296
Configuring System Auditing	298

B. Error Messages 299

About Error Messages	299
About SysMon Error Notification	300
Reference: UPS Errors	300
Reference: File-System Errors	302
Reference: RAID Errors	302
Reference: IPMI Events	303

C. Compliance Archiving Software API 305

Compliance Features	306
WORM Files	306
File Retention Periods	307
Administrative Lock-Down	307
Compliance Audit	308
Accessing Compliance Functionality	308
Compliance Volumes	309
WORM Files	309
Creating WORM Files	309
Behavior of WORM Files	310
Metadata of WORM Files	311
WORM Restrictions	311

File Retention Periods	311
Unix System Calls with Compliance Archiving	312
access(2)	313
chmod(2), fchmod(2)	313
chown(2), fchown(2)	314
link(2)	314
read(2), readv(2)	314
rename(2)	314
stat(2), fstat(2)	314
unlink(2)	315
utime(2), utimes(2)	315
write(2), writev(2)	315
Behavior of Windows Clients	315
Creating WORM Files	316
Metadata Restrictions on WORM Files	316
WORM File's Read-Only Bit	316
Compliance and Antivirus Software	316
Other APIs	317
D. Appliance and Gateway System Components	319
The Sun StorageTek 5320 NAS Server	320
Front Panel Buttons and LEDs	321
Power Button	321
Status Indicator LEDs	322
LCD Menu and Buttons	323
Back Panel Ports and LEDs	323
Back Panel LEDs	324
Server Power Supplies	325
Direct-Attached Tape Library	326

Sun StorageTek 5320 Controller Units and Expansion Units	328
Controller Units	328
Front of the Controller Unit	329
Back of the Controller Unit	330
Battery Backup Compartments	331
Expansion Units	332
Ports and Power Supplies	333
LEDs and Indicators	334
Mixed FC and SATA Capacity	335
Disk Drives	336
Identifying a Drive for Replacement	337
Locating a Drive	337
Sun StorageTek 5220 NAS Appliance	338
Back-End Storage	339
E. Sending a Diagnostic Email Message	341
F. Web Administrator Panels	345
Add LUN Wizard Panels	346
Select Controller Unit and Drives or RAID Set	346
Sun StorageTek 5320 Drive Status Indicators	347
Sun StorageTek 5300 Drive Status Indicators	348
LUN Properties	349
Confirmation Panel	350
Save Configuration	350
Antivirus Configuration Panels	350
Configure Antivirus Panel	350
Configuration Wizard Panels	352
Configuration Wizard Panel	352

Confirmation Panel	352
Select Environment Panel	353
File Replicator Panels	353
Add/Edit Mirror Window	354
Manage Mirrors Panel	355
Promote Volume Window	356
Set Threshold Alert Panel	357
View Mirror Statistics Panel	358
File Volume Operations Panels	361
Add/Edit Checkpoint Schedule Window	361
Add/Edit DTQ Setting Window	362
Add/Edit Quota Setting Window	363
Attach Segments Panel	365
Configure Directory Tree Quotas Panel	365
Configure User and Group Quotas Panel	366
Create Checkpoint Window	368
Create File Volumes/Segments Panel	369
Delete File Volumes Panel	370
Edit Volume Properties Panel	371
Manage Checkpoints Panel	373
Rename Checkpoint Window	373
Schedule Checkpoints Panel	374
New/Edit Checkpoint Schedule Panel	375
Segment Properties Window	376
View Volume Partitions Panel	377
High Availability Panels	378
Enable Failover Panel	378
Recover Panel	379

Set LUN Path Panel	380
Set Primary Path Window	381
iSCSI Configuration Panels	382
Add/Edit iSCSI Access Window	382
Add/Edit iSCSI LUN Window	383
Configure Access List Panel	385
Configure iSCSI LUN Panel	385
Configure iSNS Server Panel	386
Promote iSCSI LUN Window	386
Monitoring and Notification Panels	387
Configure SNMP Panel	388
Configure System Auditing Panel	388
Diagnostic Email Window	389
Display System Log Panel	390
Set Up Email Notification Panel	391
Set Up Logging Panel	392
Set Up UPS Monitoring Panel	394
View Fan Status Panel	394
View File Volume Usage Panel	395
View Power Supply Status Panel	396
View Temperature Status Panel	397
View Voltage Regulator Status Panel	397
Network Configuration Panels	398
Bond NIC Ports Panel	398
Configure Network Adapters Panel	400
Create/Edit Port Bond Window	403
Set Gateway Address Panel	404
Set Server Name Panel	405

Set Up DNS Panel	406
View the Routing Table Panel	407
RAID Panels	408
Add Hot-Spare Window	408
Add LUN Window	409
Locate Drive Window	411
Locate Drive Tray Window	411
Manage RAID Panel	412
View Controller/Enclosure Information Panel	414
View LUN Information Panel	415
System Activity Panels	415
View Networking Activity Panel	415
View System Activity Panel	416
System Backup Panels	417
Set Up NDMP Panel	417
System Manager Panels	418
Edit NFS Export Window	418
Server Properties Window	419
Volume Properties Window	419
System Operations Panels	420
Online System Registration	421
Activate Options Panel	422
Add License Window	423
Assign Language Panel	424
Enable Temporary Licenses Window	424
Import Licenses Window	425
Set Administrator Password Panel	425
Set Remote Access Panel	426

Set Time and Date Panel	427
Set Up Time Synchronization Panel	428
Shut Down the Server Panel	430
Update Software Panel	431
Unix Configuration Panels	432
Add/Edit Comment Window	432
Add/Edit Host Window	433
Add/Edit NFS Export Window	433
Add Hostgroup Member Window	435
Add Hostgroup Window	435
Configure Exports Panel	436
Configure Name Services Panel	437
Remove NFS Export Window	438
Set Up FTP Panel	439
Set Up Hostgroups Panel	439
Set Up Local Hosts Panel	440
Set Up NIS Panel	441
Set Up NIS+ Panel	442
Set Up NSSLDAAP Panel	443
Windows Configuration Panels	443
Add/Edit Group Panel	444
New Share Window	444
Edit Share Window	446
Add/Edit SMB/CIFS User or Group Map Window	449
Configure Autohome Panel	450
Add/Edit Rule	451
Configure Domains and Workgroups Panel	452
Configure Groups Panel	454

Configure Mapping Policy Panel 455

Configure Maps Panel 456

Configure Shares Panel 457

Remove Share Window 459

Set Up WINS Panel 459

System Status Panel 460

Index 463

Figures

FIGURE 1-1	Main Window	4
FIGURE 1-2	Navigation Panel	6
FIGURE 1-3	Expanding a Folder in the Navigation Panel	6
FIGURE 1-4	Content Panel	8
FIGURE 1-5	Status Panel	9
FIGURE 2-1	Single-Server System Configuration	18
FIGURE 2-2	Dual-Server System Configuration	19
FIGURE 5-1	Dual-Server Port Bonding	83
FIGURE 10-1	Display System Log Panel	159
FIGURE 12-1	Location of Power/OK LED	219
FIGURE 12-2	Removing the Main Cover	220
FIGURE 12-3	Removing the Front Bezel	222
FIGURE 12-4	Removing the Front Cover	223
FIGURE 12-5	Replaceable Component Locations	224
FIGURE 12-6	Opening the Fan Bay Door and Removing a Fan Module	226
FIGURE 12-7	Removing the Fan Connector Board Securing Screw	226
FIGURE 12-8	Releasing the Fan Connector Board	227
FIGURE 12-9	Removing the Front Panel Indicator Board Screws	228
FIGURE 12-10	Removing the Front Panel Indicator Board	229
FIGURE 12-11	Designations of Power Supplies	229

FIGURE 12-12	Removing a Power Supply	230
FIGURE 12-13	Designation of DIMM Slots	232
FIGURE 12-14	Removing a DIMM	233
FIGURE 12-15	Fan Connector Boards and Fan Modules Viewed from Front of Server	234
FIGURE 12-16	Opening the Fan Bay Door and Removing a Fan Module	234
FIGURE 12-17	Removing the Rear Fan Tray	235
FIGURE 12-18	PCI Slot Designations and Speeds	237
FIGURE 12-19	Opening a PCI Card Securing Latch	238
FIGURE 12-20	Removing a PCI-Card Filler Panel	238
FIGURE 12-21	Installing a PCI Card	239
FIGURE D-1	Sun StorageTek 5320 NAS Server Front View	320
FIGURE D-2	NAS Server Front Panel Buttons and LEDs	321
FIGURE D-3	NAS Server Back Panel With Single HBA Card	323
FIGURE D-4	Server Back Panel LEDs	324
FIGURE D-5	Power Supply Modules	326
FIGURE D-6	Sun StorageTek 5320 Controller Unit Battery Backup Compartment LEDs	331
FIGURE D-7	Sun StorageTek 5320 Expansion Unit Ports and Components	333
FIGURE D-8	Sun StorageTek 5320 Expansion Unit LEDs and Indicators	334
FIGURE D-9	Sun StorageTek 5320 Fibre Channel Drive Shuttles	336
FIGURE D-22	Sun StorageTek 5220 NAS Appliance, Front	338
FIGURE 4-23	Sun StorageTek 5220 NAS Appliance With Single HBA Card, Back	338

Tables

TABLE 1-1	Toolbar Icons	5
TABLE 1-2	Folder Symbols	7
TABLE 1-3	Other Buttons	7
TABLE 1-4	Help Tabs	10
TABLE 1-5	Help Icons	10
TABLE 3-1	Supported Hardware Configurations – Sun StorageTek 5310 and Sun StorageTek 5320 Appliances	42
TABLE 3-2	Sun StorageTek 5320 RAID-5 Configuration	42
TABLE 3-3	Sun StorageTek 5300 RAID-5 Configuration	43
TABLE 4-1	Supported Antivirus Scan Engine Software	71
TABLE 5-1	Dual-Server Port Bonding Example	83
TABLE 7-1	Fields in the SID	103
TABLE 8-1	Umask Access Permissions With DOS Read-Only Attribute Set	115
TABLE 9-1	Audit Log Format	150
TABLE 10-1	System Status Display	157
TABLE 10-2	System Event Icons	159
TABLE 10-3	Acceptable Voltage Ranges	164
TABLE 11-1	Time Zone Database Files	188
TABLE 11-2	CATIA Character Translation Table	190
TABLE 11-3	Component Firmware Directories and Files	198
TABLE 12-1	Supported PCI Card Part Numbers	236

TABLE A-1	Console Menu Keyboard Functions	243
TABLE B-1	UPS Error Messages	300
TABLE B-2	File-System Errors	302
TABLE B-3	RAID Error Messages	302
TABLE B-4	IPMI Error Messages	303
TABLE C-1	WORM File Metadata That Can and Cannot Be Modified	311
TABLE D-1	Sun StorageTek 5300 RAID-5 Possible Configurations	326
TABLE D-2	Sun StorageTek 5320 RAID-5 Possible Configurations	329
TABLE D-3	Battery Backup Compartment LEDs	332
TABLE F-1	Fields and Elements on the Select Controller Unit and Drives or RAID Set Panel	346
TABLE F-2	Sun StorageTek 5320 Drive Status Indicators (Add LUN)	347
TABLE F-3	Sun StorageTek 5300 Drive Status Indicators (Add LUN)	348
TABLE F-4	Fields and Elements on the LUN Properties Panel	349
TABLE F-5	Fields and Elements on the Configure Antivirus Panel	350
TABLE F-6	Fields and Elements on the Select Environment Panel	353
TABLE F-7	Fields and Elements on the Add/Edit Mirror Window	354
TABLE F-8	Fields and Elements on the Manage Mirrors Panel	355
TABLE F-9	Fields and Elements on the Promote Volume Window	356
TABLE F-10	Fields and Elements on the Set Threshold Alert Panel	357
TABLE F-11	Fields and Elements on the View Mirror Statistics Panel	358
TABLE F-12	Fields and Elements on the Add/Edit Checkpoint Schedule Window	361
TABLE F-13	Fields and Elements on the Add/Edit DTQ Setting Window	362
TABLE F-14	Fields and Elements on the Add/Edit Quota Setting Window	364
TABLE F-15	Fields and Elements on the Attach Segments Panel	365
TABLE F-16	Fields and Elements on the Configure Directory Tree Quotas Panel	366
TABLE F-17	Configure User and Group Quotas Panel	367
TABLE F-18	Fields and Elements on the Create Checkpoint Window	368
TABLE F-19	Fields and Elements on the Create File Volumes/Segments Panel	369
TABLE F-20	Fields and Elements on the Delete File Volumes Panel	370
TABLE F-21	Fields and Elements on the Edit Volume Properties Panel	371

TABLE F-22	Fields and Elements on the Manage Checkpoints Panel	373
TABLE F-23	Fields and Elements on the Rename Checkpoint Window	374
TABLE F-24	Fields and Elements on the Schedule Checkpoints Panel	374
TABLE F-25	Fields and Elements on the New/Edit Checkpoints Schedule Panel	376
TABLE F-26	Fields and Elements on the Attach Segments Panel	376
TABLE F-27	Fields and Elements on the View Volume Partitions Panel	377
TABLE F-28	Fields and Elements on the Enable Failover Panel	378
TABLE F-29	Fields and Elements on the Recover Panel	380
TABLE F-30	Fields and Elements on the Set LUN Path Panel	380
TABLE F-31	Fields and Elements on the Set Primary Path Window	381
TABLE F-32	Fields and Elements on the Add/Edit iSCSI Access Window	382
TABLE F-33	Fields and Elements on the Add/Edit iSCSI LUN Window	384
TABLE F-34	Fields and Elements on the Configure Access List Panel	385
TABLE F-35	Fields and Elements on the Configure iSCSI LUN Panel	385
TABLE F-36	Fields and Elements on the Configure iSNS Server Panel	386
TABLE F-37	Fields and Elements on the Promote iSCSI LUN Panel	387
TABLE F-38	Fields and Elements on the Configure SNMP Panel	388
TABLE F-39	Fields and Elements on the Configure System Auditing Panel	389
TABLE F-40	Fields and Elements on the Diagnostic Email Window	389
TABLE F-41	Fields and Elements on the Display System Log Panel	390
TABLE F-42	Fields and Elements on the Set Up Email Notification Panel	391
TABLE F-43	Fields and Elements on the Set Up Logging Panel	392
TABLE F-44	Fields and Elements on the Set Up UPS Monitoring Panel	394
TABLE F-45	Fields and Elements on the View Fan Status Panel	394
TABLE 4-2	Sun StorageTek 5320 NAS Appliance Server Fan Identification	395
TABLE F-46	Fields and Elements on the View File Volume Usage Panel	395
TABLE F-47	Fields and Elements on the View Power Supply Status Panel	396
TABLE F-48	Fields and Elements on the View Temperature Status Panel	397
TABLE F-49	Fields and Elements on the View Voltage Regulator Status Panel	397
TABLE F-50	Fields and Elements on the Bond NIC Ports Panel	398

TABLE F-51	Fields and Elements on the Configure Network Adapters Panel	400
TABLE F-52	Fields and Elements on the Create/Edit Port Bond Window	403
TABLE F-53	Fields and Elements on the Set Gateway Address Panel	405
TABLE F-54	Fields and Elements on the Set Server Name Panel	405
TABLE F-55	Fields and Elements on the Set Up DNS Panel	406
TABLE F-56	Fields and Elements on the View the Routing Table Panel	407
TABLE F-57	Drive Images and Buttons in the Add Hot-Spare Window	409
TABLE F-58	Sun StorageTek 5210 Add LUN Drive Status Indicators	409
TABLE F-59	Fields and Buttons on the Add LUN Window	410
TABLE F-60	Fields and Buttons on the Locate Drive Window	411
TABLE F-61	Fields and Buttons on the Locate Drive Tray Window	412
TABLE F-62	Fields and Elements on the Manage RAID Panel	413
TABLE F-63	Fields and Elements on the View Controller/Enclosure Information Panel	414
TABLE F-64	Fields and Elements on the View LUN Information Panel	415
TABLE F-65	Fields and Elements on the View Networking Activity Panel	416
TABLE F-66	Fields and Elements on the View System Activity Panel	416
TABLE F-67	Fields and Elements on the Set Up NDMP Panel	417
TABLE F-68	Fields and Elements on the Edit NFS Export Window	418
TABLE F-69	Fields and Elements on the Server Properties Window	419
TABLE F-70	Fields and Elements on the Volume Properties Window	419
TABLE F-71	Fields and Elements on the Online System Registration Panel	421
TABLE F-72	Fields and Elements on the Activate Options Panel	422
TABLE F-73	Fields and Elements on the Add License Window	423
TABLE F-74	Fields and Elements on the Assign Language Panel	424
TABLE F-75	Fields and Elements on the Enable Temporary Licenses Window	424
TABLE F-76	Fields and Elements on the Enable Temporary Licenses Window	425
TABLE F-77	Fields and Elements on the Set Administrator Password Panel	426
TABLE F-78	Fields and Elements on the Set Remote Access Panel	426
TABLE F-79	Fields and Elements on the Set Time and Date Panel	427
TABLE F-80	Fields and Elements on the Set Up Time Synchronization Panel	428

TABLE F-81	Fields and Elements on the Shut Down the Server Panel	430
TABLE F-82	Fields and Elements on the Update Software Panel	431
TABLE F-83	Fields and Elements on the Add/Edit Comment Window	432
TABLE F-84	Fields and Elements on the Add/Edit Host Window	433
TABLE F-85	Fields and Elements on the Add/Edit NFS Export Window	433
TABLE F-86	Fields and Elements on the Add Hostgroup Member Window	435
TABLE F-87	Fields and Elements on the Add Hostgroup Window	435
TABLE F-88	Fields and Elements on the Configure Exports Panel	436
TABLE F-89	Fields and Elements on the Configure Name Services Panel	437
TABLE F-90	Fields and Elements on the Configure Exports Panel	438
TABLE F-91	Fields and Elements on the Set Up FTP Panel	439
TABLE F-92	Fields and Elements on the Set Up Hostgroups Panel	440
TABLE F-93	Fields and Elements on the Set Up Local Hosts Panel	440
TABLE F-94	Fields and Elements on the Set Up NIS Panel	441
TABLE F-95	Fields and Elements on the Set Up NIS+ Panel	442
TABLE F-96	Fields and Elements on the Set Up NSSLDAP Panel	443
TABLE F-97	Fields and Buttons on the Add/Edit Group Window	444
TABLE F-98	Fields and Buttons on the New Share Window	445
TABLE F-99	Fields and Buttons on the Edit Share Window	447
TABLE F-100	Fields and Buttons on the Add/Edit SMB/CIFS User or Group Map Window	449
TABLE F-101	Fields and Buttons on the Configure Autohome Panel	450
TABLE F-102	Fields and Buttons on the Configure Autohome Panel	452
TABLE F-103	Configure Domains and Workgroups Panel	453
TABLE F-104	Fields and Elements on the Configure Groups Panel	454
TABLE F-105	Fields and Elements on the Configure Mapping Policy Panel	456
TABLE F-106	Fields and Elements on the Configure Maps Panel	457
TABLE F-107	Fields and Buttons on the Configure Shares Panel	458
TABLE F-108	Fields and Elements on the Remove Share Window	459
TABLE F-109	Fields and Buttons on the Set Up WINS Panel	460
TABLE F-110	Fields on the System Status Panel	460

Preface

The *Sun StorageTek NAS OS Administration Guide* is a combined administrator's and user's guide for the:

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

This guide describes how to use the Web Administrator graphical user interface (GUI) to set up and monitor your appliance or gateway system. It also includes instructions to use the command-line interface (CLI), and details about the hardware that are not documented in the NAS appliance and gateway system *Getting Started Guide*.

In general, the features described in this manual apply for all the above mentioned devices, with exceptions noted in the text, as applicable.

The Sun StorageTek 5210 NAS Appliance and the Sun StorageTek 5220 NAS Appliance are single-server appliances with storage built in to the server, so references to *cluster configurations* and *gateways systems* never apply. For the Sun StorageTek 5210 NAS Appliance, references to *controller enclosures/units* never apply. References to expansion enclosures are valid, however, if your StorEdge 5210 NAS Appliance is configured with the optional expansion enclosure.

Before You Read This Book

Before reading this guide, you must have installed and configured your appliance or gateway system as described in the *Getting Started Guide* for your NAS appliance or gateway system.

How This Book Is Organized

This guide is broken down as follows:

[Chapter 1](#) provides an overview of features for the Web Administrator graphical user interface (GUI).

[Chapter 2](#) describes basic network and file-system configuration.

[Chapter 3](#) describes file-system setup and management.

[Chapter 4](#) describes system management functions.

[Chapter 5](#) describes port settings.

[Chapter 6](#) describes naming conventions.

[Chapter 7](#) describes group, host, and file directory security settings.

[Chapter 8](#) describes shares, quotas, and exports.

[Chapter 9](#) describes licensable software options.

[Chapter 10](#) describes monitoring functions.

[Chapter 11](#) describes maintenance functions.

[Chapter 12](#) contains replacement procedures for customer-replaceable units (CRUs).

[Appendix A](#) describes using the console to perform system tasks.

[Appendix B](#) describes error messages produced by the various NAS appliance and gateway-system components.

[Appendix C](#) describes the Compliance Archiving Software API.

[Appendix D](#) describes details about the NAS hardware.

[Appendix E](#) describes how to send a diagnostic email.

[Appendix F](#) describes the Web Administrator panels.

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	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. <code>% You have mail.</code>
AaBbCc123	What you type, as contrasted with on-screen computer output.	<code>% su</code> 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 those shown here.

Related Documentation

The documents listed as online are available at:

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

Application	Title	Part Number	Format	Location
Notes & known issues	<i>Sun StorageTek NAS OS 4.21 Software Release Notes</i>	819-6652- <i>nn</i>	PDF HTML	Online
Safety	<i>Sun StorageTek 5320 NAS Array Regulatory and Safety Compliance Manual</i>	819-6048- <i>nn</i>	PDF HTML	Online
	<i>Sun StorageTek 5220 NAS Appliance Regulatory and Safety Compliance Manual</i>	819-7366- <i>nn</i>	PDF HTML	Online
	<i>Sun StorageTek 5220 NAS Array Regulatory and Safety Compliance Manual</i>	819-7367- <i>nn</i>	PDF HTML	Online
	<i>Sun StorEdge 5310 NAS Appliance Safety and Compliance Guide</i>	819-0881- <i>nn</i>	PDF HTML	Online

Application	Title	Part Number	Format	Location
Installation	<i>Sun StorEdge 5210 Expansion Unit Safety, Regulatory, and Compliance Manual</i>	817-7515- <i>nn</i>	PDF HTML	Online
	<i>Sun StorEdge 5300 RAID Expansion Unit and Sun StorEdge 5300 Expansion Unit Safety and Compliance Guide</i>	819-0882- <i>nn</i>	PDF	Online
	<i>Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide</i>	819-4283- <i>nn</i>	PDF HTML	Online
	<i>Sun StorageTek NAS OS Administration Guide</i>	819-7167- <i>nn</i>		
	<i>Sun StorEdge 5310 NAS Appliance and Gateway System Getting Started Guide</i>	819-3237- <i>nn</i>	PDF HTML	Online
	<i>Sun StorEdge 5210 NAS Hardware Installation, Configuration, and User Guide</i>	817-6660- <i>nn</i>	PDF HTML	Online
	<i>Sun StorageTek 5320 NAS Appliance Setup (Poster)</i>	819-4385- <i>nn</i>	Printed PDF	Ship kit Online
	<i>Sun StorageTek 5320 NAS Gateway System Setup (Poster)</i>	819-4286- <i>nn</i>	Printed PDF	Ship kit Online
	<i>Sun StorEdge 5310 NAS Gateway System Poster</i>	819-3240- <i>nn</i>	Printed PDF	Shipp kit Online
<i>Sun StorageTek 5220 NAS Appliance Setup</i>	819-7166- <i>nn</i>	Print PDF	Ship kit Online	

Documentation, Support, and Training

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

Third-Party Web Sites

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

Sun Welcomes Your Comments

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

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

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

Sun StorageTek NAS OS Administration Guide, part number 819-4284-10

Product Overview

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

- [“Introduction” on page 1](#)
- [“Using Web Administrator” on page 1](#)
- [“Using the Configuration Wizard” on page 11](#)
- [“Where to Go From Here” on page 13](#)

Introduction

The Web Administrator graphical user interface (GUI) makes it easy to set security and network configurations, and to perform administrative tasks on Sun Microsystems innovative NAS appliances and gateway systems.

Note: Most software features and functions described in this book apply to any configuration of the NAS appliance and gateway-system software. Where a feature or function is limited to a specific configuration, that configuration is identified specifically.

Using Web Administrator

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

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

- [“Logging In” on page 2](#)

- [“About the Interface Layout” on page 4](#)
 - [“About the Toolbar” on page 4](#)
 - [“About the Navigation Panel” on page 6](#)
 - [“About the Folder Symbol Key” on page 7](#)
 - [“About Other Buttons” on page 7](#)
 - [“About the Content Panel” on page 8](#)
 - [“About the Status Panel” on page 9](#)
 - [“Using Help” on page 10](#)
-

Logging In

The Login panel enables authorized users to access the system through the Web Administrator graphical user interface (GUI). By default, there is no password for the system administrator. If you wish to set this password, follow the directions in [“Setting the Administrator Password” on page 67](#).

Steps to Log In

To log in to the Web Administrator GUI:

1. Type the system administrator password in the Password field.
Passwords are case-sensitive. If there is no system administrator password, leave this field blank.
2. Click Apply to open the main Web Administrator display.

Considerations With Multiple Users

Web Administrator allows any number of simultaneous users, and employs a unique writer-lock mechanism to ensure that only a single GUI user can update data at a given time, while supporting concurrent read-only access to the same data. The data is locked only as long as is necessary to complete the update request. If one user is accessing data for write access and you request an update on the same data:

- If the first user’s update request is in-process, Web Administrator will notify you that the data is currently locked, and will identify the locked-by user by host-system IP address. In this case, you will have to resubmit your request (possibly after refreshing your display).

If the first user loses the connection to the NAS server before the update is finished, the lock will time-out after 30 minutes.

As necessary, the Administrator can view and reset the lock before the 30 minute time-out, using the `datalock show` and `datalock reset lock-id` CLI commands. Be careful if you do this, making sure it is safe to reset the lock.

- If the first user's update request has completed, but it may have affected the data you are looking at currently, Web Administrator will prompt you to refresh your current display. You can choose to refresh, or you can continue with your update without refreshing.

With cluster (dual-server) configurations, the data subject to update is locked on both servers simultaneously. This means that the processing described above applies whether the two users are accessing the same server, or partner servers in a cluster configuration.

Note: Avoid simultaneous updates by Telnet/CLI and Web Administrator users.

About the Interface Layout

The Web Administrator graphical user interface (GUI) is divided into sections, as shown below:

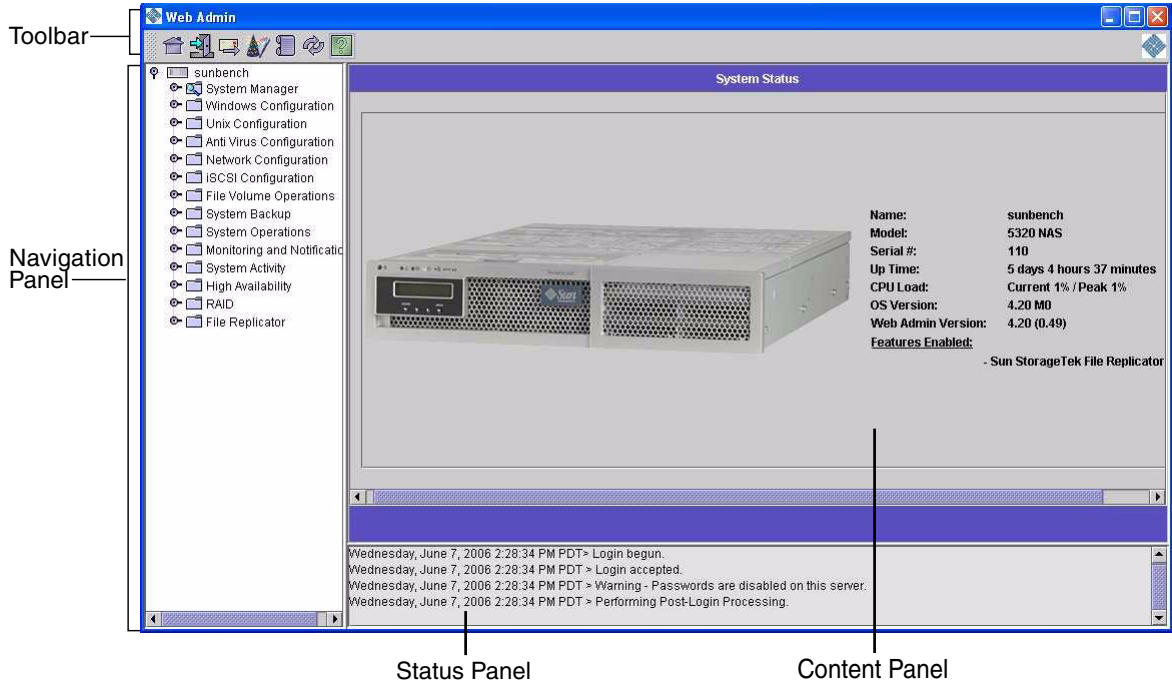
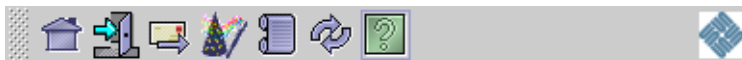


FIGURE 1-1 Main Window

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








About the Toolbar

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



The toolbar icons are detailed in [TABLE 1-1](#).

TABLE 1-1 Toolbar Icons

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

About the Navigation Panel

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

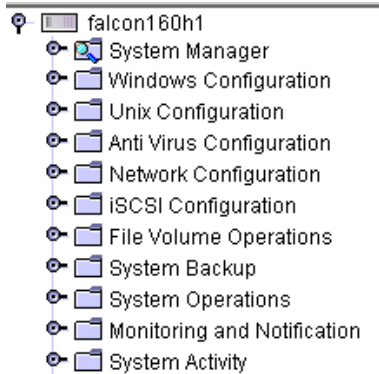



FIGURE 1-2 Navigation Panel

To open a folder, click the  symbol next to the folder, or double-click the folder.

The symbol changes to the  position, as shown in the following figure.

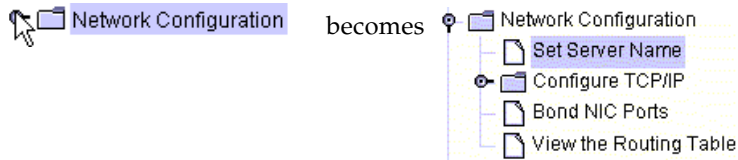












FIGURE 1-3 Expanding a Folder in the Navigation Panel

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

About the Folder Symbol Key

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

TABLE 1-2 Folder Symbols

Symbol	Description
	File volume
	Compliant file volume (with red folder tab)
	Shared file volume
	Exported file volume
	Shared and exported file volume
	Mirrored file volume (applicable only when the Sun StorageTek File Replicator option is licensed and enabled)
	Compliant mirror (applicable only when the Sun StorageTek Compliance Archiving Software and the Sun StorageTek File Replicator options are licensed and enabled)
	Segment

About Other Buttons

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

TABLE 1-3 Other Buttons






Button	Name	Action
	Add	Add an item.

TABLE 1-3 Other Buttons (Continued)

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

About the Content Panel

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



FIGURE 1-4 Content Panel

For information about system status, see [“Viewing System Status”](#) on page 157.

About the Status Panel

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

The following figure shows the status panel.



FIGURE 1-5 Status Panel

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

The status messages are stored in a local log file, in case the client application requires diagnostic action. Some or all of the messages are included in the log file, according to how the administrator configures the log file.

The name of the log file is constructed from the IP address of the client and the number of the rotating version of the file:

`n_n_n_cnt.log`

where *n* are the components of the IP address and *cnt* is 1, 2, or 3, depending on the version of the log file. The file is located in the following location:

Unix systems (user home directory)/.sun_nas_webadmin

Windows systems Documents and Settings/(user name)/.sun_nas_webadmin

Using Help

To view additional information about the Web Administrator software, click the Help button in the Web Administrator toolbar. The Help window consists of a Navigation pane on the left, and a Topic pane on the right.

To display a Help topic, use the Contents, Index, and Search tabs in the Navigation pane. Click the Search tab and click Tips on Searching to learn about the search feature.




The following table describes the Help tabs.

TABLE 1-4 Help Tabs

Tab	Description
Contents	Click a folder icon to display subtopics. Click a page icon to display the Help page for that topic in the Topic pane.
Index	Click an index entry to display the corresponding Help page.
Search	Type the words for which you want to search and click Search. The Navigation pane displays a list of topics that match your search criteria in order of relevancy. Click a topic link to display the Help page for that topic. Click the Tips on Searching link for information about how to improve your search results. To search for a particular word or phrase within a topic, click in the Topic pane, press Ctrl+F, type the word or phrase for which you are searching, and click Find.

The meanings of the Help window icons are described in the following table.

TABLE 1-5 Help Icons

Control/Indicator	Description
	Go back to the previous Help topic that you viewed in the current session.
	Go forward to the next Help topic that you viewed in the current session.
	Print the current Help topic.

Using the Configuration Wizard

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

About Configuration Wizard Variations

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

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

The wizard can take either of three primary paths. The path you use is based on your network environment:

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

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

Running the Wizard

To run the configuration wizard:

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

The wizard is launched in a separate window.

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

The wizard progresses through several steps, which are detailed starting with [“Initial Network Configuration” on page 15](#). The steps are as follows:

- Setting the server name and contact information
- Configuring network adapters
- Setting the default gateway
- Configuring Domains and Workgroups (Windows environments and mixed environments) and enabling and configuring Active Directory Service (ADS) (Windows environments and mixed environments)
- Configuring Windows Internet Naming Service (WINS) (Windows environments and mixed environments)
- Setting up Domain Name Service (DNS)

Note: If the system boots using Dynamic Host Configuration Protocol (DHCP), confirm that the address of the DNS server is correct. If not, clear the Configure DNS checkbox to avoid delays in restarts and failovers.

- Setting up Network Information Service (NIS) (Unix environments and mixed environments)
- Setting up Network Information Service Plus (NIS+) (Unix environments and mixed environments)
- Configuring name services (Unix environments and mixed environments)
- Setting up email notification
- Setting up remote and local logging
- Assigning the language

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

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

If you do not want to run the wizard, [“Initial Network Configuration” on page 15](#) describes accessing the same functions in the same sequence through the navigation panel.

Where to Go From Here

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

Establishing your file system includes defining any logical unit numbers (LUNs), partitions, file volumes, and segments that you need to set. For more information about these concepts, see [“File-System Concepts” on page 39](#).

When your file system is complete, you must set up user access rights and any other system management features. [“System Management” on page 67](#) covers the basic management functions. View the index to find any specific features, including descriptions of the features, how they work, when and why they apply, and any specific rules for setting them up.

Initial Network Configuration

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

- [“About the Initial Network Configuration” on page 16](#)
- [“Setting the Server Name” on page 16](#)
- [“Managing LUN Paths” on page 17](#)
- [“Enabling Failover” on page 21](#)
- [“Initiating Failback \(Recovery\)” on page 23](#)
- [“Configuring Network Ports and Adapters” on page 24](#)
- [“Setting the Default Gateway Address” on page 27](#)
- [“Managing Name Services” on page 27](#)
- [“Setting Up Email Notifications” on page 34](#)
- [“Setting Up Logging” on page 35](#)
- [“Assigning the Language” on page 36](#)
- [“Backing Up Configuration Information” on page 37](#)
- [“Where to Go From Here” on page 37](#)

About the Initial Network Configuration

The Web Administrator graphical user interface (GUI) enables you to configure your system for communication on your network. After you configure network communication and services, you need to configure your file system, user access rights, any other features, and any options that you purchased.

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

Setting the Server Name

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

To set the server name:

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

The server name identifies the system or identifies the server unit, for dual-server high-availability (HA) systems on the network. The server name begins with a letter of the alphabet (a-z, A-Z) or number 0-9 and can include up to 30 characters: a-z, A-Z, 0-9, hyphens (-), underscores (_), and periods (.).

3. Type the contact information for your company.

The system includes this information in any diagnostic email messages that it sends. For more information about diagnostic email messages, see [“Sending a Diagnostic Email Message” on page 341](#).

4. Click Apply to save your settings.

Managing LUN Paths

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

- [“About Setting LUN Paths” on page 17](#)
- [“About LUN Paths in Single-Server Systems” on page 18](#)
- [“About LUN Paths in Dual-Server Systems” on page 19](#)
- [“Setting LUN Paths” on page 20](#)
- [“Restoring a LUN Path” on page 21](#)

About Setting LUN Paths

A logical unit number (LUN) path is a designation that describes how a file volume in a LUN is accessed by which NAS server and controller. To every file volume there are two LUN paths from the NAS server controllers to the disk array controllers: primary and alternate. If one fails, the system uses the other available LUN path to access the desired file volume. The number of LUN paths and their implementations depend on the model and configuration of the system. In a cluster configuration, a server (head) induces a head failover (see [“Enabling Server Failover” on page 22](#)) if both the primary and alternate paths fail.

For more information, see [“Setting LUN Paths” on page 20](#).

About LUN Paths in Single-Server Systems

FIGURE 2-1 shows a single-server appliance or gateway configuration.

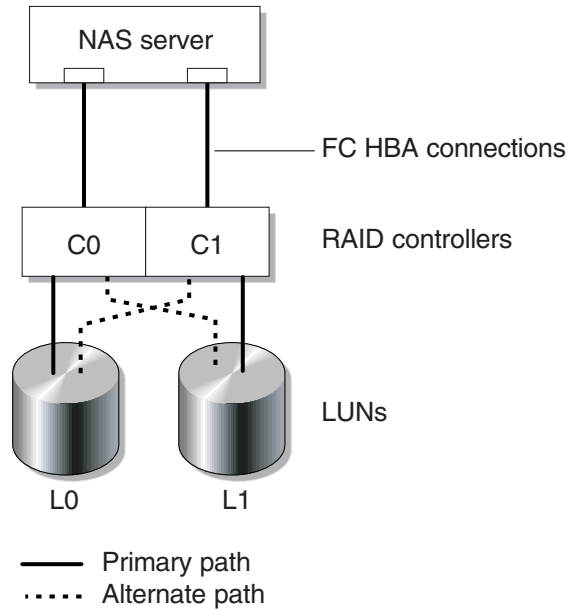


FIGURE 2-1 Single-Server System Configuration

The primary logical unit number (LUN) path to a file volume in L0 (:LUN 0) is C0-L0, and the alternate path is C1-L0. The primary LUN path to a volume in L1 is C1-L1, and the alternate path is C0-L1. As illustrated above, the system has the following LUN paths.

Paths	LUN 0	LUN 1
Primary	C0-L0	C1-L1
Alternate	C1-L0	C0-L1

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

About LUN Paths in Dual-Server Systems

FIGURE 2-2 shows a cluster appliance or gateway system configuration.

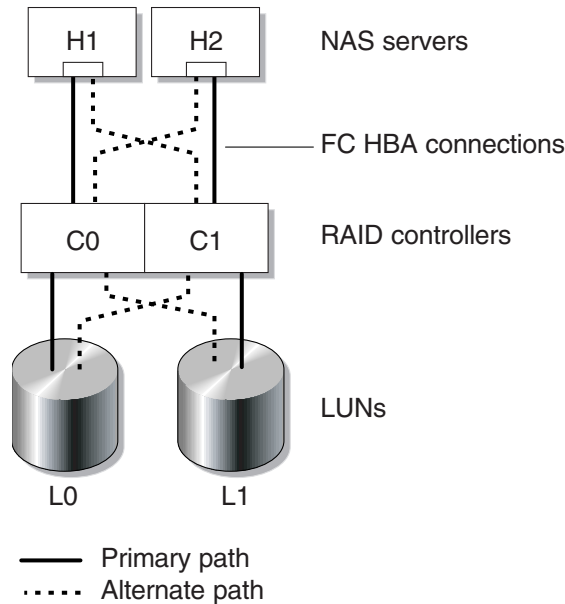


FIGURE 2-2 Dual-Server System Configuration

The primary logical unit number (LUN) path to L0 (LUN 0) path on server H1 is C0-L0; the alternate path is C0-L1. The primary L0 path on server 2 is C1-L0 and the alternate path is C1-L1.

File volumes are normally accessed through the primary LUN path designated for the LUN to which the file volumes belong. In a cluster configuration, a server induces a failover if its primary and alternate paths fail (see [“Enabling Server Failover”](#) on page 22).

Setting LUN Paths

By setting a logical unit number (LUN) path, you designate the current active LUN path. The current active LUN path can be either the primary or alternate path. For optimal performance, set the active path to the primary path. A LUN can be reassigned only if there are no file systems on that LUN. On a cluster appliance, only the server that “owns” a LUN can reassign it to another server.

Note: When you first start a cluster appliance, all LUNs are assigned to one server (H1). Use server H1 to reassign some LUNs to server H2 for even distribution of data. The global limit (for both servers, combined) is 255 LUNs. This limit can be divided between the two servers in any way. For example, you might have 200 LUNs on one server, and 56 on the partner server.

You use the Set LUN Path panel to set active paths. For a cluster appliance, you can set an unassigned path from either server.

You can specify the primary and alternate path for each LUN, or you can have the paths assigned automatically by clicking the Auto-assign LUN paths button in the Set LUN Paths window.

Note: The Sun StorEdge 5310 NAS Appliance Version 4.5 documentation set does not show the graphic user interface’s change from Fault Tolerance to High Availability. When a procedure in that documentation instructs you to select Fault Tolerance, select High Availability.

To set a LUN path:

1. From the navigation panel, choose High Availability > Set LUN Path.

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

2. Select a LUN and click Edit.
3. Select the controller that you want from the Primary Path drop-down menu.

Example: The drop-down option “1/0” assigns the selected LUN to controller 0 (C0). The option value is X/Y, where X is the HBA and Y is the controller ID (SID) through which the LUN is seen by the NAS server.

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

Restoring a LUN Path

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

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

To restore a LUN path:

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

If you are restoring the primary LUN path because of a physical path failure, scan the disks to make the alternate path available again. To rescan the disks, use the Web Administrator to navigate to Volume Operations > Create File Volumes and then click Scan for New Disks.

Enabling Failover

This section provides information about enabling server failover on Sun StorageTek 5310 and Sun StorageTek 5320 cluster appliances and cluster gateway systems. The following subsections are included:

- [“About Enabling Failover” on page 21](#)
- [“Enabling Server Failover” on page 22](#)

About Enabling Failover

Note: Failover processing is only available on Sun StorageTek 5310 and Sun StorageTek 5320 cluster appliances and cluster gateway systems. It does not apply for Sun StorageTek 5210 NAS appliances.

A cluster appliance or gateway system includes a pair of active-active servers, sometimes called *heads*, that share access to the redundant array of independent disks (RAID) controllers and several different networks. The RAID controllers are connected to each server through Fibre Channel controllers. A dedicated heartbeat cable connects the first network interface card (NIC) between the two servers and lets each server monitor the other's health status.

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

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

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

You can initiate the recovery process, known as "failback," when the failed server is repaired and brought back online. This is described under "[Initiating Recovery](#)" on page 24.

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



Caution: In a cluster configuration, do not configure both heads to be in the same switch zone as the tape device. In the event of a head failover during a backup, data on the media is lost. Configure one of the heads to be in the same zone as the tape device.

Enabling Server Failover

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

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

To enable head failover:

1. From the navigation panel, choose High Availability > Enable Failover.
2. Select the Automatic Failover checkbox.
3. Select the Enable Link Failover checkbox.

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

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

Initiating Failback (Recovery)

This section provides information about manually initiating failback (recovery) for a cluster appliance or cluster gateway system, in the event that a failed server is brought back online. It applies for Sun StorageTek 5310 and Sun StorageTek 5320 cluster appliances and cluster gateway systems, and includes the following subsections:

- [“About Initiating Recovery” on page 24](#)
- [“Initiating Recovery” on page 24](#)

About Initiating Recovery

After a failed server is brought back online and fully functional, you must manually initiate recovery (failback) of your cluster appliance or gateway system. This allows the server that originally failed to “recover” ownership of its original file volumes.

For example, if volume A was assigned to server H1, which failed, server H2 would take ownership of volume A during the failover process. When server H1 is fully functional again, you can log in to server H2 and return ownership of volume A to server H1.



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

Initiating Recovery

After a cluster appliance or cluster gateway system has undergone head failover, and the failed server is brought back online, you must manually initiate recovery (failback) of the server that was brought back up.

To initiate recovery:

1. Log in to Web Administrator on the server that took over for the failed server.
Note: You cannot initiate recovery from the failed (and now, recovered) server.
2. From the navigation panel, choose High Availability > Recover.
3. Click Recover. (Ignore the redundant array of independent disks (RAID) lists at the center of the screen; they are not used during server recovery.)

Under a heavy processing load, some LUNs might not be fully restored. Repeat the procedure if any LUN remains in the failover state.

Configuring Network Ports and Adapters

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

- [“About Configuring Network Ports” on page 25](#)
- [“About Network Port Locations” on page 25](#)
- [“Configuring Network Adapters” on page 25](#)

About Configuring Network Ports

Each network port on your NAS appliance or gateway system must have an assigned role. Take either of the following actions to configure network ports on your NAS appliance or gateway system:

- Enable Dynamic Host Configuration Protocol (DHCP).
- Specify the Internet Protocol (IP) address, netmask, broadcast, and network interface card (NIC) port role for each network port through the Configure Network Adapters panel. You can also use this panel to 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 [“About Port Bonding” on page 79](#).

About Network Port Locations

The NAS appliance and gateway-system ports are identified based on their type, and their physical and logical location on the server. To identify the network port locations, see [“Back Panel Ports and LEDs” on page 323](#) and the NAS appliance and gateway system *Getting Started Guide*. Note that configurations vary, and those shown are examples.

The relationship of network interface cards (NICs) to ports is also shown in the *Getting Started Guide* for your NAS appliance or gateway system.

Configuring Network Adapters

To configure network adapters:

1. From the navigation panel, choose Network Configuration > Configure TCP/IP > Configure Network Adapters.

2. If your network uses a Dynamic Host Configuration Protocol (DHCP) server to assign Internet Protocol (IP) addresses and you want to enable it, select the Enable DHCP checkbox.

Enabling DHCP allows the system to dynamically acquire an IP address from the DHCP server. Clear this checkbox to manually specify a static IP address and netmask. If you do not enable DHCP, the netmask is still disabled if the port is a member of an aggregate port. See [“About Port Bonding” on page 79](#) for more information on creating and setting up aggregate ports.

Note: On cluster appliances and gateway systems, you cannot enable DHCP unless you have disabled head failover. Instead, you must assign static IP addresses to ports so that they remain consistent in the event of a failover.

3. From the Adapter list, select the port you want to configure.

If you have already created a port bond and want to add alias IP addresses to it, select the port bond from this list. (See [“About Port Bonding” on page 79](#) for more information on creating port bonds.) Independent ports are labelled PORTx and port bonds are labelled BONDx.

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

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

5. Type the IP subnet mask for the selected port or port bond.

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

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

6. Select one of the following roles for each port, referring to [“About Port Locations and Roles” on page 77](#) for details:

Roles	Description of the Port
Primary	Active network port. At least one port must be assigned a primary role.
Independent	Active network port used for purposes other than serving data, such as backups.
Mirror	Port that connects the server to another server for purposes of mirroring file volumes (applicable only with the Sun StorageTek File Replicator option is licensed and enabled).

Roles	Description of the Port <i>(Continued)</i>
Private	Port reserved for the heartbeat: a dedicated network link that constantly monitors the status of the other server in a cluster configuration (applicable only in dual-server configurations). Each server in a cluster configuration has one and only one private port.

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

Typically aliases specify the IP addresses of obsolete systems that have been replaced by NAS storage.

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

- Repeat [Step 3](#) through [Step 7](#) for all ports in the Adapter list.
- Click Apply to save your changes.

Setting the Default Gateway Address

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

To set the default gateway address:

- From the navigation panel, choose Network Configuration > Configure TCP/IP > Set Gateway Address.
- Type the gateway address in the Gateway text box.
- Click Apply to save your settings.

Managing Name Services

This section provides information about setting up Windows security so that name services can be used, and provides information about setting up various name services. For more detailed information about name services, see [“Active Directory Service and Authentication” on page 85](#). The following subsections are included:

- [“Configuring Windows Security” on page 28](#)
 - [“Setting Up WINS” on page 29](#)
 - [“Setting Up DNS” on page 30](#)
 - [“Setting Up NIS” on page 31](#)
 - [“Setting Up NIS+” on page 32](#)
 - [“Configuring Name Services” on page 34](#)
-

Configuring Windows Security

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

Note: In a cluster configuration, Windows security changes made on one server are propagated immediately to the other server.

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

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

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

To configure Windows security:

1. From the navigation panel, choose Windows Configuration > Configure Domains and Workgroups.
2. To enable Windows domain security, select the Domain option, and fill in the Domain, User Name, and Password fields to create an account on the domain for this server.

You must specify a user account with rights to add servers to the specified domain. For more information about these fields, see [“Configure Domains and Workgroups Panel” on page 452](#).

3. To enable Windows workgroup security, select the Workgroup option, and type 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, type a description of the NAS appliance or gateway system.
5. To enable ADS, select the Enable ADS checkbox and fill in the ADS-related fields. For more information about these fields, see [“Configure Domains and Workgroups Panel” on page 452](#).
For more detail about ADS, refer to [“About Active Directory Service” on page 86](#).
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, choose System Operations > Set Time and Date from the navigation panel.
6. Click Apply to save your settings.
If you change the security mode from workgroup to NT domain, or from NT domain to workgroup, the server reboots when you click Apply.

Setting Up WINS

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

Follow the steps below to set up WINS:

Note: In a cluster configuration, WINS changes made on one server are propagated immediately to the other server.

1. From the navigation panel, choose Windows Configuration > Set Up WINS.
2. To enable WINS, select the Enable WINS checkbox.
Checking this box makes the system a WINS client.
3. Type the Internet Protocol (IP) address of the Primary WINS server in the space provided.
The primary WINS server is the server consulted first for NetBIOS name resolution.
4. Type the Secondary WINS server in the space provided.
If the primary WINS server does not respond, the system consults the secondary WINS server.
5. (Optional) Type the NetBIOS Scope identifier in the Scope field.

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

6. Click Apply to save your settings.

Setting Up DNS

Domain Name Service (DNS) software resolves host names to Internet Protocol (IP) addresses for your NAS appliance or gateway system.

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

Follow the steps below to set up DNS:

Note: In a cluster configuration, DNS changes made on one server are propagated immediately to the other server.

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

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

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

5. To rearrange the search order of the DNS servers in the list, click 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 NAS appliance or gateway system into the DNS namespace.

Do not enable this option if your DNS server does not accept dynamic updates. You must also configure the Kerberos realm and KDC server in [“Configuring Windows Security” on page 28](#). If you enable Dynamic DNS by selecting this checkbox, non-secure dynamic updates occur automatically if they are allowed by the DNS server.

7. To enable secure Dynamic DNS updates, select the Enable Dynamic DNS checkbox and fill in the DynDNS User Name and DynDNS Password fields. For more information about these fields, see [“Set Up DNS Panel” on page 406](#).
8. Click Apply to save your settings.

Setting Up NIS

Network information service (NIS) is a name service that enables the distribution of system configuration data, such as user and host names, between computers in a computer network. This is a UNIX function so if you are running a pure Windows network, you do not need to set up NIS.

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

Follow the steps below to set up NIS:

Note: In a cluster configuration, NIS changes made on one server are propagated immediately to the other server.

1. From the navigation panel, choose Unix Configuration > Set Up NIS.
2. Select the Enable NIS checkbox.

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

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

Use the DNS naming convention (for example, `domain.com`).

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

This is the server from which the database is imported.

Leave the Server field blank if you do not know the server IP address. However, if you leave the Server field blank, you must select the Use Broadcast checkbox so that the appropriate IP address can be acquired from the NIS server.

5. Type 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 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 name service that provides the same functionality as NIS, but with added security that ensures a secure environment. This is a UNIX function, so if you are running a pure Windows network, do not set up NIS+.

Note: The commands and structure of NIS+ are different from NIS.

Note: In a cluster configuration, NIS+ changes made on one server are propagated immediately to the other server.

Setting up NIS+ is a two-phase process:

1. Adding the NAS appliance or gateway system to the host credential file.
2. Configuring NIS+.

To add an appliance or gateway system to the host credential file on the NIS + server:

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

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

where *server* is the name of the NAS server, and *domain* is the name of the NIS+ domain that the appliance or gateway system is joining.

Note: Include a period at the end of the domain name only after the **-P** argument. For example, if a NAS appliance is named **SS1**, and its NIS+ domain is **sun.com**, enter:

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

3. At the prompt, enter a password. This password will be used again later in this procedure.

To configure NIS+:

1. From a remote client, open a web browser window to the system and log in to Web Administrator.
2. From the navigation panel, choose Unix Configuration > Set Up NIS+.
3. Select the Enable NIS+ checkbox.
4. In the Home Domain Server field, type 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 acquires the appropriate IP address for the home domain server.
5. In the NIS+ Domain field, type the NIS+ home domain.
Note: NIS+ domain names must end with a period (".").
6. Type the secure RPC password for the NIS+ server.
Use the password that you set earlier in this procedure.
7. Type the search path as a colon-separated list of domains.
The search path identifies the domains that NIS+ searches through when looking for information. Leave this space empty to search only the home domain and its parents.
For example, if the NIS+ domain is `eng.sun.com.` and the search path is blank, the system first searches `eng.sun.com.` then `sun.com.`, and so on, when resolving names. Conversely, if you specify a search path like `sun.com.`, the system searches only the domain `sun.com` when resolving names.
8. Select the Use Broadcast checkbox if you do not know the IP address of the home domain server (see [Step 5](#)).
9. Click Apply to save your settings.

Configuring Name Services

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

Follow these steps to set the order for user, group, netgroup, and host lookup:

Note: In a cluster configuration, changes made on one server to user, group, netgroup, and host look-up are propagated immediately to the other server.

1. From the navigation panel, choose Unix Configuration > Configure Name Services.
2. Select the order of user lookup in the Users Order tab by selecting a service from the Services Not Selected box and using the > and < buttons, and then use the Up and Down buttons in the Services Selected box.
3. Select the services used for group lock-up in the Groups Order tab, following the procedure in [Step 2](#).
4. Select the services used for netgroup lock-up in the Netgroup Order tab, following the procedure in [Step 2](#).
5. Select the services used for host lock-up in the Hosts Order tab, following the procedure in [Step 2](#).
6. Click Apply to save your changes.

Setting Up Email Notifications

When the system detects an error, it sends a notification email message. To ensure name resolution, you must have either set up the SMTP server host name in the Configure Hosts panel (see [“About Configuring Hosts” on page 98](#)) or set up DNS (see [“Setting Up DNS” on page 30](#)).

Follow these steps to set up SMTP and send email messages to the recipients:

Note: In a cluster configuration, SMTP changes made on one server are propagated immediately to the other server.

1. From the navigation panel, choose Monitoring and Notification > Set Up Email Notification.

2. Type the name of the SMTP server that you want to use to send notification.
3. In the Email Address field, type the address of the person to be notified of system errors.
4. Specify the types of email for this recipient. Select Notification, Diagnostics, or both.
5. Click the Add button to add the new recipient to the List of recipients.
6. Repeat [Step 3](#) through [Step 5](#) for all recipients. You can specify a maximum of four email addresses.
To remove someone from the list, select the address and click the Trash button.
7. Select the notification level.
8. Click Apply to save your settings.

Setting Up Logging

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



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

To set up remote and local logging:

1. From the navigation panel, choose Monitoring and Notification > View System Events > Set Up Logging.
2. Select the Enable Remote Syslogd box.
3. In the Server field, specify the DNS host name if you have configured the DNS settings. Otherwise, type the Internet Protocol (IP) address. This is where the system log is sent.
4. From the drop-down menu, select the facility code to be assigned to all NAS messages that are sent to the log.

5. Select the types of system events for which to generate log messages, by placing a check mark next to one or more facilities. Each type of event represents a different priority, or severity level, as described under [“About System Events” on page 159](#).
6. To set up a local log, check Enable Local Log.
7. Type the log file’s path (the directory on the system where you want to store the log file) and file name in the Local File field.
Note: You cannot set up local logging to either the /cvol or /dvol directory.
8. Type the maximum number of archive files in the Archives field.
The allowable range is from 1 to 9.
9. Type the maximum file size in kilobytes for each archive file in the Size field.
The allowable range is from 100 to 999,999 kilobytes.
10. Click Apply to save your settings.

Assigning the Language

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

To assign the language:

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

Registering the System

You can register your Sun account and NAS server information with Sun Services online. If you do not have a Sun Account, you can create one during the registration.

To register the system:

1. From the navigation panel, choose System Operations > Online System Registration.

2. Read Sun's privacy policy and disclaimer. To continue, click the Agree button.
3. If you do not have a Sun Account, click on the [here](#) link at the bottom of the dialog. This opens the Sun Online Account Registration portal Click Register to begin to create the account.
4. If you have a Sun Account, type its ID in the Sun Account ID and enter its password.
5. Click Next to go to the Proxy Server tab.
6. Enter the name of the proxy server you want Sun Services to use and its port number. If the proxy server uses authentication, enter its user name and its password.
7. Click Next to go to the Options tab.
8. Select the type of information you want to send to Sun Services. The heartbeat data is a periodic check without regard to the type of event. The fault events are sent when a failure is occurring.
9. Click Apply to save your changes.

Backing Up Configuration Information

After you have completed the system configuration, back up the configuration information in the event of a system failure. For information about backing up configuration information, see [“Backing Up Configuration Information” on page 191](#).

Where to Go From Here

At this point, your system is in full communication with the network. However, before your users can begin storing data, you must set up the file system and establish user access rights. For more information, see [“File-System Setup and Management” on page 39](#).

To set up quotas, shares, exports, or other access controls, see [“Shares, Quotas, and Exports” on page 113](#).

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 NAS appliances and gateway systems. It includes the following sections:

- [“File-System Concepts” on page 39](#)
- [“Creating the File System” on page 46](#)
- [“Creating File Volumes or Segments” on page 50](#)
- [“About Rebuilding a LUN” on page 55](#)
- [“Managing File Volumes and Segments” on page 55](#)
- [“Configuring the NAS for iSCSI” on page 59](#)
- [“Where to Go From Here” on page 65](#)

File-System Concepts

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

- [“About RAID Configurations” on page 40](#)
- [“About LUNs” on page 43](#)
- [“About Partitions” on page 44](#)
- [“About File Volumes” on page 45](#)
- [“About Segments” on page 45](#)

About RAID Configurations

There are different redundant array of independent disks (RAID) system configurations that are supported by the system. The following sections describe these configurations:

- [“About RAID Systems” on page 40](#)
- [“About the RAID-0 Configuration \(Not Supported\)” on page 40](#)
- [“About the RAID-1 Configuration \(Gateway Systems Only\)” on page 41](#)
- [“About the RAID-1+0 Configuration \(Gateway Systems Only\)” on page 41](#)
- [“About the RAID-5 Configuration” on page 41](#)
- [“NAS RAID-5 Systems – Sun StorageTek 5310 and Sun StorageTek 5320 Appliances” on page 42](#)

About RAID Systems

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

There are multiple types of RAID configurations. NAS appliances support RAID 5 only. NAS gateway systems support RAID 1, RAID 1+0, and RAID 5.

About the RAID-0 Configuration (Not Supported)

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

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

About the RAID-1 Configuration (Gateway Systems Only)

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

About the RAID-1+0 Configuration (Gateway Systems Only)

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

About the RAID-5 Configuration

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

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

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

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

NAS RAID-5 Systems – Sun StorageTek 5310 and Sun StorageTek 5320 Appliances

[TABLE 3-1](#) summarizes the supported hardware configurations for Sun StorageTek 5310 and Sun StorageTek 5320 and appliances.

TABLE 3-1 Supported Hardware Configurations – Sun StorageTek 5310 and Sun StorageTek 5320 Appliances

NAS Server	Supported Controller Units/Enclosures	Supported Expansion Units/Enclosures
5320 NAS Server	Sun StorageTek 5320 Controller Unit	Sun StorageTek 5320 Expansion Unit
	Sun StorageTek 5300 Controller Enclosure	Sun StorageTek 5300 Expansion Enclosure
5310 NAS Server	Sun StorageTek 5300 Controller Enclosure	Sun StorageTek 5300 Expansion Enclosure

Each Sun StorageTek 5320 controller unit and expansion unit contains either 8 or 16 redundant array of independent disks (RAID) drives of a single drive type (either Fibre Channel (FC), or Serial Advanced Technology Attachment (SATA)). The Sun StorageTek 5320 devices are configured as shown in [TABLE 3-2](#).

TABLE 3-2 Sun StorageTek 5320 RAID-5 Configuration

Per Expansion Unit or Controller Unit	RAID-5 Set	Volumes	Hot-Spare
8 drives	6+1	1 if using FC 300 GB drives	1
		2 of equal size for all other drives	
16 drives	6+1	1 if using FC 300 GB drives	1
		2 of equal size for all other drives	
	7+1	2 of equal size	

Each 5300 expansion enclosure contains either 7 or 14 RAID drives of a single drive type (either FC or SATA), configured as shown in [TABLE 3-3](#). Sun StorageTek 5300 controller enclosures can contain drives as long as they are FC drives, in which case they are also configured as shown in [TABLE 3-3](#). The 5300 controller enclosure cannot contain SATA drives.

TABLE 3-3 Sun StorageTek 5300 RAID-5 Configuration

Per Expansion Enclosure or Controller Enclosure (FC only)	RAID-5 Set	Volumes	Hot-Spare
7 drives	5+1	1	1
14 drives	5+1	1	1
	6+1	1 if using FC drives 2 of equal size if using 400GB SATA drives	

NAS RAID-5 Systems – Sun StorageTek 5210 Appliances

For Sun StorageTek 5210 NAS appliances, the server contains either one or two RAID controllers, and slots for seven drives. As shipped by the manufacturer, six of the seven slots contain SCSI drives that are configured as a single 4+1 SCSI RAID-5 set (with two logical unit numbers (LUNs)), plus one hot-spare.

Optionally, you can connect up to three expansion enclosures (JBODs) with the server, each containing either 6 or 12 drives.

About LUNs

Management of the NAS storage resources is accomplished through the logical unit number (LUN), with little direct management of the redundant array of independent disks (RAID) sets themselves. See [“About Creating RAID Sets and LUNs” on page 46](#) for directions and more information on setting up both RAID sets and LUNs.

A logical unit number (LUN) is the logical representation of a storage area within a RAID set. NAS appliances and gateway systems support a maximum of 255 LUNs. For cluster configurations, the 255-LUN limit is shared across both servers (for example, 100 LUNs on one server, and 156 on the partner server).

There is a maximum size limit per LUN of 2 terabytes (TB). This limit is imposed by the underlying storage protocol used to access the LUN.

In versions of NAS software earlier than 4.20, NAS in-band RAID management (IBRM) did not allow for the creation of multiple LUNs (also known as *volumes*) per RAID set, which resulted in wasted space on RAID sets that exceeded 2 terabytes. (For LUNs that were pre-built at the factory, there could be more than one LUN per RAID set, and the multiple LUNs were displayed and managed correctly by the NAS OS.)

Starting with NAS software version 4.20, you can create more than one LUN for each RAID set, thereby making use of space that would otherwise be wasted. This is sometimes referred to as *LUN carving*. To access more than 2 terabytes in a single RAID set, you can define as many LUNs as necessary to carve out the size you want.

About Partitions

Partitions are sections on a logical unit number (LUN) and provide a way to subdivide the total space available within a LUN. The NAS software supports a maximum of 31 partitions per LUN. Partitions are defined automatically when you create a LUN.

Note – New components are now configured with LUNs during manufacturing so you must initialize the partition table manually before they can be used. On the File Volume Operations page, a LUN with a partition table displays a white block, indicating free space, and the value 1 as the number of partitions. A LUN without a partition table displays a blank block and does not display the number of partitions.

When a LUN is first created, all of the available space is allocated to 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 adjusted to match the size of the file volume and any additional space on the LUN is assigned to the next partition. After you have made all of the file volumes the operating system supports, any extra space on that LUN is inaccessible.

About File Volumes

File volumes define the spaces that are available for storing information, and are created from partitions that have available space. If the volume does not use up all the available space in a partition, the remaining space is allocated into the next partition. New file volumes are limited to 256 gigabyte in size. To create a larger file volume, you can create and attach up to 63 segments (see [“About Segments” on page 45](#)) to the original file volume.

You can increase the size of a file volume by attaching a segment (see [“About Segments” on page 45](#)). The segment is essentially another file volume with special characteristics. When you add a segment to an existing volume, there is no distinction between the two and a user sees only more space in the volume. This flexibility 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. As a system administrator adds drives and LUNs, user see more space within the 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 might involve adding more drives and/or expansion units; however, the user sees only more storage space.

About Segments

Segments are “volumes” of storage space created much like file volumes. They can be attached to an existing file volume at any time. Attaching a segment increases the original file volume’s total capacity. Each segment must be created independently and then attached to a file volume. After the segment is 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. After the segment is attached to the original file volume, the different physical storage locations are invisible to the user. Therefore, space can be added as needed, without bringing down the network to restructure the data storage and create a bigger file volume.

Creating the File System

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

- [“About Creating the File System” on page 46](#)
 - [“About Creating RAID Sets and LUNs” on page 46](#)
 - [“Adding a New LUN \(Sun StorageTek 5310 and Sun StorageTek 5320 NAS Devices\)” on page 48](#)
 - [“Adding a New LUN \(Sun StorageTek 5210 NAS Appliances\)” on page 49](#)
 - [“Designating a Drive As a Hot-Spare” on page 49](#)
-

About Creating the File System

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

If you are configuring a (non-gateway) appliance, refer to [“About Creating RAID Sets and LUNs” on page 46](#) and [“Designating a Drive As a Hot-Spare” on page 49](#).

About Creating RAID Sets and LUNs

NAS appliances and gateway systems support a maximum of 255 logical unit numbers (LUNs). For cluster configurations, the 255-LUN limit is shared across both servers, but can be split any way.

The NAS software uses two approaches to creating new redundant array of independent disks (RAID) sets and LUNs, depending on your hardware:

- For Sun StorageTek 5310, 5320, and 5220 NAS appliances, a LUN wizard steps you through the process of creating new LUNs. New LUNs can be defined in either an existing RAID set (a RAID set that already has one or more LUNs defined), or a new RAID set (in which case the wizard creates the RAID set with the LUN).

- For Sun StorageTek 5210 NAS appliances, which include an LSI MegaRAID controller, you can create only one LUN per RAID set. For these devices, the NAS software combines the creation and definition of RAID sets with the definition of the (LUN), simplifying the process of establishing both. In effect, you create both simultaneously.

Before you add a new LUN, verify the following:

- Before creating a LUN, make sure the drives not assigned to another LUN and that they are not assigned to another function, for example, as a hot-spare drive.
- **Caution:** In a cluster appliance, each server manages its own LUNs. Verify that failover is enabled and configured for both servers. See [“About Enabling Failover” on page 21](#) for details.



After you add a new LUN, check the following:

- If the LUN was deleted and then reintroduced to the NAS appliance using a method other than In-Band RAID Management, you must reboot the appliance. A reboot is not required in Gateway systems. You can unmap and remap the LUN as described in the *Sun StorEdge 5310 NAS Appliance and Gateway System Administration Guide*.
- When you assign a LUN to each server in a gateway cluster configuration, you must manually scan the disk on both servers to pick up the new LUNs. You can scan for new disks using Web Admin in one of two ways:
 - Right-click System Manager in the navigation pane and choose Scan for New Disks
 - Go to File Volume Operations → Create File Volumes in the navigation panel and click Scan for New Disks on the Create File Volumes panel

If the new LUN had been assigned to another host in the SAN and is now added to the NAS Gateway system, the LUN might be inaccessible because it has residual data, indicated by having an owner of “no DPMGR.” To remove the data and make the LUN usable, use the following procedure:

- Verify that the proper LUN has been added to the NAS Gateway system and make sure that the data on the LUN is not important or valuable.
- Run the following CLI command to clear the data. This command reformats the LUN:

```
hostname> disk disk-name,partition-number zap
```

Caution: The zap command reformats the LUN. The disk table will be deleted.



Adding a New LUN (Sun StorageTek 5310 and Sun StorageTek 5320 NAS Devices)

For Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances, a wizard steps you through the process of creating new logical unit numbers (LUNs). New LUNs can be defined either in an existing redundant array of independent disks set (a RAID set that already has one or more LUNs defined), or a new RAID set. When a LUN is created in a new RAID set, the wizard creates the RAID set as well as the LUN.

1. From the navigation panel, choose RAID > Manage RAID.
2. Click Add LUN to launch the wizard, then follow the prompts as it guides you through the process of creating the new LUN and, as applicable, the new RAID set (detailed in [Step 3](#) through [Step 5](#)).
3. When prompted to select the controller unit, use the Controller Unit drop-down menu to select the controller unit that will manage the new LUN.
4. When prompted to select the physical drives for the LUN (same screen as for [Step 3](#)), you can use unassigned drives, or you can select an existing RAID set. If you use unassigned drives, select at least three drives from the graphical image on the right. Each drive image is keyed to indicate whether it is available for use, selected already for LUN membership, empty, and so forth. Refer to [“Select Controller Unit and Drives or RAID Set” on page 346](#) for details.
5. In the LUN Properties window, specify the LUN size (up to 2 terabytes), the server that manages the LUN (applicable only for cluster (dual-server) configurations). Then select the radio button that describes how to proceed:
 - Create New File Volume – Create the new LUN on the physical drives or RAID set selected, and create a new file system on that LUN. Specify the name of the new file volume. Refer to [“About Partitions” on page 44](#) and [“About File Volumes” on page 45](#) for details.
 - Grow Existing File Volume – Create a LUN on the physical drives or RAID set selected, and use that LUN to expand the storage for an existing file system. Select that file system from the drop-down menu.
 - None – Create the new LUN, but do not create a file system on the LUN.

Adding a New LUN (Sun StorageTek 5210 NAS Appliances)

For Sun StorageTek 5210 NAS appliances, follow these steps to create a new logical unit number (LUN) and redundant array of independent disks (RAID) set:

1. From the navigation panel, choose RAID > Manage RAID.
2. Click Add LUN.
3. From the Controller drop-down menu, select the number of the controller to which you want to add a LUN.
4. Select the drives that will belong to the LUN by clicking each drive image.
You must select at least three drives. The drive images show the status of each drive. For information about the drive images and their statuses, see [“Add LUN Window” on page 409](#).
5. Select one of the following volume options:
 - Create New Volume – Select this option to create a new volume for this LUN. The entire LUN will be used to create the volume. Type the name of the new volume in the space provided.
Note: In a cluster configuration, volume names must be unique across cluster members.
 - Grow Existing File 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 drop-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 and build the RAID set.

Designating a Drive As a Hot-Spare

You can configure any drive as a hot-spare for NAS appliances.

To designate a drive as a hot-spare:

1. From the navigation panel, choose 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.

The drive images show the status of each drive, as detailed under [“Add Hot-Spare Window” on page 408](#). Make sure the disk you select as a hot-spare is at least as large as the largest disk in any logical unit number (LUN) defined on the NAS appliance.

4. Click Apply to add the new hot-spare.

Creating File Volumes or Segments

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

- [“About Creating a File Volume or a Segment” on page 50](#)
- [“Creating a File Volume or Segment Using the Create File Volumes Panel” on page 51](#)
- [“Creating a File Volume or Segment Using the System Manager” on page 52](#)
- [“Attaching Segments to a Primary File Volume” on page 53](#)

About Creating a File Volume or a Segment

New file volumes are limited to 256 gigabyte in size. To create a larger file volume, you can add segments to the primary volume. You create one primary volume and then attach up to 63 segments to increase its size.

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

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

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

1. From the navigation panel, choose File Volume Operations > Create File Volumes.
 - a. Select a LUN file volume from the list.
 - b. Click Initialize Partition Table.
 - c. Repeat Steps a and b for all uninitialized LUNs.
2. If you have recently added new disks to the live system without performing a reboot, click the Scan For New Disks button.

The partition number for the file volume in the Partition drop-down menu will increment when the file volume is created.

3. Type in the name of the new volume or segment in the Name field.

The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 12 alphanumeric characters (a-z, A-Z, 0-9).

Note: In a cluster configuration, volume names must be unique across cluster members. Identical volumes names cause problems in the event of failover. See [“About Enabling Failover” on page 21](#) for more information.

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

The total space available is shown beneath this field.
6. Select the file volume type (Primary, Segment, or Raw).
7. If you have the Sun StorageTek 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.

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

Caution: After 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 269](#) for more information.

For more information, see [“About the Compliance Archiving Option” on page 147](#).

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

Note: After creating a volume, you must create a share for the volume. Users can then access the volume and create directories. After directories are created on the volume, you can create individual shares for them.

Creating a File Volume or Segment Using the System Manager

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

1. From the navigation panel, right-click System Manager.
2. Choose Create Volume or Create Segment from the pop-up menu to open the desired window.
3. In the LUN box, click the logical unit number (LUN) where you want to create the primary file volume. If the LUN has not been initialized, indicated by a blank display, use the following procedure to initialize the LUN's partition table:
 - a. Select the LUN file volume from the list.
 - b. Click Initialize Partition Table.
 - c. Repeat Steps a and b for all uninitialized LUNs.

The partition number for the file volume in the Partition drop-down menu will increment when the file volume is created.

4. Type in the name of the new volume or segment in the Name field.

The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 12 alphanumeric characters (a-z, A-Z, 0-9).
5. Select whether the size of the file volume is reported in MB (megabytes) or GB (gigabytes) by clicking on the drop-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, Segment, or Raw).
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: After 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 269](#) for more information.

For more information, see [“About the Compliance Archiving Option” on page 147](#).

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

Note: After creating a volume, you must create a share for the volume. Users can then access the volume and create directories. After directories are created on the volume, you can create individual shares for them.

Attaching Segments to a Primary File Volume

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

- [“About Attaching Segments to a Primary File Volume” on page 54](#)
- [“Attaching a Segment Using the Attach Segments Panel” on page 54](#)
- [“Attaching a Segment Using the System Manager” on page 54](#)

About Attaching Segments to a Primary File Volume

Attaching segments to a primary file volume expands the size of the volume. The segment becomes permanently associated with the volume and cannot be removed. You must create a segment before you can attach it to a volume. Refer to [“About Creating a File Volume or a Segment” on page 50](#) for instructions.



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

A file volume by itself is limited to 256 gigabytes; however, up to 63 segments from any logical unit number (LUN) can be attached to any file volume. Each segment can be as small as 8 megabytes and as large as 256 gigabytes.

You can attach a segment using the Attach Segments panel, or the System Manager software.



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

Attaching a Segment Using the Attach Segments Panel

To attach a segment by using the Attach Segments panel:

1. From the navigation panel, choose File Volume Operations > Attach Segments.
2. Click to select the desired volume from the Existing Volumes box.
3. Click to select the desired segment from the Available Segments box.
4. Click Apply to attach.

Attaching a Segment Using the System Manager

To attach a segment by using the System Manager software:

1. From the navigation panel, click System Manager to view existing volumes.
2. Right-click the desired file volume to access the pop-up menu, then select Attach Segment.

3. For each segment that you want to attach, select the desired segment and click Apply to attach it.
Only one segment can be selected and attached at a time.

About Rebuilding a LUN

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

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

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

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

Managing File Volumes and Segments

File-system management tasks include the following:

- [“Editing File Volume Properties” on page 56](#)
- [“Deleting File Volumes or Segments” on page 58](#)
- [“Viewing Volume Partitions” on page 58](#)
- [“System Language Considerations” on page 59](#)

Editing File Volume Properties

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

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

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

1. From the navigation panel, choose File Volume Operations > Edit Properties.
2. From the Volumes list, select the name of the volume you want to change.
3. If you wish to change the volume name, type the new name.

The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 12 alphanumeric characters (a-z, A-Z, 0-9).

4. To exclude the volume from virus scans, select Virus Scan Exempt.
5. If you plan to maintain file-volume checkpoints, or to run NDMP backups, select Enable Checkpoints. Checkpoints are enabled by default when you first create a file volume.

Note: If you clear this checkbox, any checkpoints taken already will be deleted immediately, regardless of their defined retention.

6. With checkpoints enabled, select one or both of the checkpoint options.:

Option	Description
Use for Backups	Select this box if you plan to create NDMP backups for the file volume. NDMP performs backups from a copy of the file volume, thereby avoiding potential problems involved with backing up from the live file system.
Automatic	Select this box if you plan to create checkpoints for the file volume. After selecting this box, the NAS software allows you to schedule regular checkpoints, as described under “Scheduling File-System Checkpoints” on page 178 .

7. Select Enable Quotas to enable quotas for the selected volume. Quotas are disabled by default when you create a file volume.
8. Select Enable Attic to temporarily save deleted files in the.attic\$ directory located at the root of each volume. By default, this option is enabled.

In rare cases on very busy file systems, the .attic\$ directory can be filled faster than it processes deletes, leading to a lack of free space and slow performance. In such a case, disable the .attic\$ directory by clearing this checkbox

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



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



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

For more information, see [“About the Compliance Archiving Option” on page 147.](#)

Option	Description
Mandatory Enforcement	If the volume is compliance-enabled with mandatory enforcement, you cannot change to advisory enforcement.
Advisory Enforcement	If the volume is compliance-enabled with advisory enforcement and you want to change the volume to be compliance-enabled with mandatory enforcement, you can change the setting by selecting Mandatory Enforcement.
Permanent Retention	Default. If you do not want the data permanently retained, you must select the Retain for <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 the data is 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.

10. Click Apply to save your changes.

Deleting File Volumes or Segments

In some instances, after deleting files, volume free space does not change, most likely due to the checkpoint feature or the attic enable feature. (For information about attic enabling, see [“Editing File Volume Properties” on page 56.](#))

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 has expired, a maximum of two weeks. An exception occurs with manual checkpoints, which are retained indefinitely.

If you need to delete files to free disk space on a full volume, you must remove or disable checkpoints. Otherwise, you will be unable to delete the files. Refer to [“Removing a Checkpoint” on page 181](#) for instructions on removing checkpoints.

Note: Compliance-enabled volumes with mandatory enforcement cannot be deleted, and volumes or LUNs that are off-line cannot be deleted.

To delete a file volume or segment:

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

Viewing Volume Partitions

The View Volume Partitions panel is a read-only display of the logical unit numbers (LUNs) defined for the NAS appliance or gateway system. It applies for single- and dual-server (cluster) configurations.

To view volume partitions:

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

System Language Considerations

The NAS software stores file and directory names internally in the file system, using 8-bit Unicode Transformation Format (UTF-8) encoding. If you use names that are not UTF-8 encoded, the NAS software converts them to UTF-8 before passing the name to the file system. This allows your client applications to store the files on NAS storage, and to share the files between Unix and Windows applications.

- For Windows clients, which use standard Unicode, the NAS software always converts the names to UTF-8.
- For NFS clients using standard 7-bit US-ASCII or UTF-8, no conversion is required.
- For all other NFS clients, the NAS software performs name conversion if the client is identified as belonging to either the *iso8859* or *euc-kr* host group. These host groups are predefined to support name translation.

If you have NFS clients that fall into either of the categories below, follow the steps described to enable file/directory name translation:

- NFS clients that use one of the standardized multilingual single-byte coded (8-bit) graphic character sets defined by ISO 8859. Add these clients to the *iso8859* host group to enable name translation, referring to [“Adding a Member to a Host Group” on page 101](#) for detailed instructions.
- NFS clients that use the EUC-KR Extended Unix Code (EUC) 8-bit character encoding system for file/directory names that are in Korean (as for locales *ko*, *ko_KR.EUC*, or *ko_KR.euckr*). For these clients:
 - a. Add the NFS client to the *euc-kr* host group, referring to [“Adding a Member to a Host Group” on page 101](#) for detailed instructions.
 - b. Make sure the system language is set to Korean, referring to [“Assigning the Language” on page 36](#) for detailed instructions.

Configuring the NAS for iSCSI

This section provides information about configuring a NAS appliance or gateway system to expose storage on NAS file volumes as Internet Small Computer Systems Interface (iSCSI) logical unit numbers (LUNs), thereby making them available to iSCSI initiator applications running on host clients. It contains the following subsections:

- [“About iSCSI” on page 60](#)
- [“About Configuring an iSCSI Target” on page 62](#)

- [“Creating an iSCSI Access List” on page 62](#)
 - [“Creating an iSCSI LUN” on page 63](#)
 - [“About iSCSI Target Discovery Methods” on page 64](#)
-

About iSCSI

Internet Small Computer Systems Interface (iSCSI) is a transport protocol that allows host system applications to access storage devices by encapsulating and sending SCSI commands, data, and status information over TCP/IP (Transmission Control Protocol/Internet Protocol) networks. iSCSI employs a client-initiator/server-target model, where an iSCSI initiator (host-system application) encapsulates SCSI packets and sends them to a target storage device (the server).

NAS appliances and gateway systems can be configured to process Internet Small Computer Systems Interface (iSCSI) commands, and to make NAS storage available to iSCSI applications running on host clients. The NAS appliance or gateway system acts as the iSCSI target in this case, for one or more iSCSI initiator clients (host applications).

The current implementation supports the following iSCSI initiators:

- Microsoft Software Initiator
- Solaris 10 Initiator, update 3
- Linux Redhat 4 U3
- QLogic HBA on Microsoft

For Microsoft applications, NAS iSCSI supports:

- SQL database
- Exchange
- iSCSI software boot for Windows
- Microsoft Qlogic iSCSI HBA boot

Each iSCSI logical unit number (LUN) can be shared by any number of client initiators, if the client applications and operating systems recognize the disk is being shared. In addition, the NAS iSCSI software supports up to four simultaneous connections per session (that is, between each client initiator and a single iSCSI LUN), for load balancing and/or high availability.

The means, for example, that if the client application is Microsoft Exchange, and several MS Exchange servers are clustered to manage the same MS Exchange database, each server (up to four) can have a connection to the same iSCSI storage on the NAS device.

After you enable iSCSI, iSCSI initiators can store and access data on the NAS file systems just like any other client application. To facilitate this, you define iSCSI logical unit numbers (LUNs) within standard NAS file systems. These iSCSI LUNs use an area of dedicated storage (a file) to emulate a SCSI disk device, providing physical storage for data processed by iSCSI client applications. This storage is treated:

- By iSCSI, as a raw storage device.
- By the NAS appliance or gateway system, as any other file, with full benefit of:
 - Redundant array of independent disks (RAID) storage systems
 - Failover (in a cluster configuration)
 - Remote replication, including replication of iSCSI configuration data such as iSCSI LUNs and access lists), as well as replication of application data (see [“About the Sun StorageTek File Replicator Option” on page 132](#)).
 - Enforcement of compliance archiving guidelines (see [“About the Compliance Archiving Option” on page 147](#)).
 - Checkpoints (see [“” on page 171](#)).

The iSCSI target implemented on NAS appliances and gateway systems is based on iSCSI RFC 3720, developed by the Internet Engineering Task Force (IETF). The supported protocol features include:

- Header digest.
- Data digest.
- Initiator Challenge Handshake Authentication Protocol (CHAP).
- Error recovery levels 0, 1, and 2.

About iSCSI Identifiers

Each iSCSI initiator and target has a unique, permanent identifier.

The iSCSI initiator identifier is generated by iSCSI software on the host initiator.

The iSCSI target identifier is generated when you create iSCSI logical unit numbers (LUNs), using this IQN format:

```
iqn.1986-03.com.sun:01:mac-address.timestamp.user-specified-name
```

where:

- The *mac-address* is the network address of the LUN.
- The *timestamp* is the number of seconds after 1/1/1970 in hexadecimal format.
- The *user-specified ame* is the name given to the LUN when it was created.

About Configuring an iSCSI Target

Follow these steps to configure the NAS appliance or gateway system as an iSCSI target. This allows iSCSI initiators (host applications) to connect to, and access, iSCSI logical unit numbers (LUNs) on the NAS device:

1. Configure the iSCSI initiator client, referring to the documentation provided with the iSCSI initiator software.
2. Create one or more access lists, each comprising a list of iSCSI initiators that can access a specific set of iSCSI LUNs on the NAS device. Refer to [“Creating an iSCSI Access List” on page 62](#) for further details. You will associate the appropriate access list with each LUN during LUN definition.
3. Configure one or more iSCSI LUNs, each corresponding to an area of storage on the NAS device that will be accessible to iSCSI clients. Refer to [“Creating an iSCSI LUN” on page 63](#) for further details. Assign the appropriate access list to each LUN, to identify those iSCSI initiators that can access it.
4. Configure the iSCSI target discovery method, referring to [“About iSCSI Target Discovery Methods” on page 64](#) for further details.

Creating an iSCSI Access List

An Internet Small Computer Systems Interface (iSCSI) access list defines a set of iSCSI initiators that can access one or more iSCSI logical unit numbers (LUNs) on the NAS device.

Follow these steps to create or edit an iSCSI access list:

1. From the navigation panel, choose iSCSI Configuration > Configure Access List.
2. Click Add to open the Add iSCSI Access window, or select an existing access list and click Edit to modify the list.
3. Fill in the fields to define the access list, specifying the name of the access list, the name of the Challenge Handshake Authentication Protocol (CHAP) initiator and password, and the client initiators that belong to the list. CHAP ensures that the incoming data is sent from an authentic iSCSI initiator. For detailed information about the fields, see [“Add/Edit iSCSI Access Window” on page 382](#).
4. Click Apply to save the settings.

Creating an iSCSI LUN

To configure the NAS appliance or gateway system as an Internet Small Computer Systems Interface (iSCSI) target, you must configure one or more iSCSI logical unit numbers (LUNs) that will be accessible to iSCSI clients. Each iSCSI LUN uses a dedicated storage area (on a standard NAS file volume) to provide physical storage for data processed by iSCSI client applications.

iSCSI LUNs provide optimal performance if the volumes they reside on are used exclusively for iSCSI LUNs. If these volumes also contain Common Internet File System (CIFS) shares or Network File System (NFS) mounts, the performance of the iSCSI LUNs might not be optimal (depending on the I/O traffic of each protocol).

Before adding or editing an iSCSI LUN, ensure that you have created the corresponding access list for the LUN. For more information, see [“Creating an iSCSI Access List” on page 62](#).



Caution: You can configure more than one iSCSI initiator to access the same target LUN; however, the applications running on the iSCSI client server must ensure synchronized access to avoid data corruption.

Follow these steps to create an iSCSI LUN:

1. From the navigation panel, choose iSCSI Configuration > Configure iSCSI LUN.
2. Click Add to open the Add iSCSI LUN window, or select an existing iSCSI LUN and click Edit to modify a LUN definition.
3. Fill in the fields to define the iSCSI LUN, specifying the LUN name (and optional alias), the corresponding NAS file volume, LUN capacity (maximum of 2 terabytes), whether the LUN is thin-provisioned, and the access list. For detailed information about the fields, see [“Add/Edit iSCSI LUN Window” on page 383](#).
4. Click Apply to save the settings.

About SCSI Thin-Provisioned LUNs

As a general rule when creating Small Computer Systems Interface (SCSI) logical unit numbers (LUNs), configure fully provision LUNs if sufficient storage is available.

If you create thin-provisioned (that is, *sparse*) iSCSI LUNs, disk space is not allocated prior to use. Thin-provisioned LUNs are useful when you expect to define several iSCSI LUNs that will not use their full capacity. For example, when you expect that five LUNs of 100 gigabytes each will use only 55% of their capacity, you can create

them all on a file volume that can hold $5 \times 100 \times .55 = 275$ gigabytes (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 to use the majority of the storage allocated for iSCSI LUNs, do not configure thin provisioning. Some operating environments do not handle out-of-space conditions gracefully on thin-provisioned LUNs, so it's best to use full provisioning for optimal system behavior.

About iSCSI Target Discovery Methods

An Internet Small Computer Systems Interface (iSCSI) initiator can locate its iSCSI NAS target using any of the following methods:

- Static configuration – Manually add the iSCSI target name or Internet Protocol (IP) address to the iSCSI initiator host, referring 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, referring to the documentation provided with your iSCSI initiator software for details. The initiator will issue a SendTargets request to discover the list of accessible iSCSI targets.



Caution: Advertise each iSCSI LUN only once on the network. Do not advertise the same iSCSI Qualified Name (IQN) from two different NAS devices. (This could happen with mirroring, after promoting a copy of the file on a mirror volume.)

- Internet Storage Name Service (iSNS) server – Set up a 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. iSNS facilitates device discovery across Fibre Channel storage area networks, as well in IP storage networks.

Support for an iSNS server is an optional feature, and can be configured using the Web Administrator GUI, as described under [“Specifying an iSNS Server” on page 65](#).

Specifying an iSNS Server

Follow these steps to enable use of an Internet Storage Name Service (iSNS) server for iSCSI target discovery. The NAS iSNS client inter-operates with any standard iSNS server, such as Microsoft iSNS Server 3.0.

To specify the iSNS server:

1. From the navigation panel, choose iSCSI Configuration > Configure iSNS Server.
2. Identify the iSNS server to use, specifying either the server's Internet Protocol (IP) address or Domain Name Service (DNS) name.
3. Click Apply to save the setting.

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 back up 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.

This chapter includes the following sections:

- [“Setting the Administrator Password” on page 67](#)
- [“Controlling the Time and Date” on page 68](#)
- [“Using Antivirus Software” on page 70](#)

Setting the Administrator Password

By default, there is no password for the system administrator. Follow the steps below to set this password, as desired. In a cluster configuration, changes made to the administrator password on one server are propagated immediately to the other server.

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

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

4. Type the new password again in the Confirm Password field.
To disable a password, leave the New Password and Confirm Password fields blank.
5. Click Apply to save your changes.

Controlling the Time and Date

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

- [“About Controlling the Time and Date” on page 68](#)
- [“About Time Synchronization” on page 68](#)
- [“Setting Up Time Synchronization” on page 69](#)
- [“Setting the Time and Date Manually” on page 70](#)

About Controlling the Time and Date

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

About Time Synchronization

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

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

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

Setting Up Time Synchronization

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

To set up time synchronization:

1. From the navigation panel, choose System Operations > Set Up Time Synchronization.
2. Select one of the following three options:
 - **Manual Synchronization** – Select this option if you do not want to use either NTP or RDATE time synchronization.
 - **NTP Synchronization** – Select this option if you want to use NTP synchronization and have at least one NTP server on the network.
For detailed information about the NTP Synchronization options, see [“Set Up Time Synchronization Panel” on page 428](#).
 - **RDATE Synchronization** – Select this option if you want to set up the RDATE server and tolerance window.
For detailed information about the RDATE Synchronization options, see [“Set Up Time Synchronization Panel” on page 428](#).
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. From the navigation panel, choose System Operations > Set Time and Date.
2. Select the correct year from the drop-down menu above the calendar and to the left.
3. Select the correct month from the drop-down menu above the calendar and to the right.
4. Click the correct date in the calendar.
5. Select the correct hour from the drop-down list box above the clock and to the left. The values range from 0 (midnight) to 23 (11:00 p.m.).
6. Select the correct minute (0 to 59) from the drop-down menu above the clock and to the right.
7. Select the correct time zone from the drop-down menu at the bottom of the screen.

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

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

Using Antivirus Software

This section provides information about using antivirus software. The following subsections are included:

- [“About Virus Scanning” on page 71](#)
- [“Enabling Antivirus Protection” on page 72](#)

About Virus Scanning

Data can be protected by real-time virus scanning using off-system scan engines. If a connection to a scan engine fails, the file is sent to another available scan engine. If another scan engine is not available, the scan fails and access to the file might be denied. You can exempt some data from virus scanning.

Note: Only CIFS file systems can be scanned. NFS and FTP files are not scanned by any scan engine.

TABLE 4-1 shows the antivirus software that is supported.

TABLE 4-1 Supported Antivirus Scan Engine Software

antivirus Software	ICAP Support	NAS OS Version
Symantec antivirus Scan Engine 4	Yes	4.12, 4.20, 4.21
Symantec antivirus Scan Engine 5	Yes	4.20, 4.21
Computer Associates eTrust AntiVirus 7.1	No*	4.20, 4.21
Trend Micro Interscan Web Security Suite (IWSS) 2.5	Yes	4.21

* Requires installation of the “Sun StorageTek 5000 NAS ICAP Server v3.0 for Computer Associates eTrust Antivirus Scan Engine” that can be downloaded free from <http://www.sun.com/download/> and searching on the product.

A file is scanned during Common Internet File System (CIFS) open and close file operations if the file has not been scanned with the current virus definitions or if it has been modified since last scanned.

If a virus is detected, the system log records the name of the infected file, the name of the virus, and the action taken for the file. In most cases, the action is to deny access to the file. The only allowed action is to delete the file. In addition to the system log, details of the infections are recorded in a virus log file that resides in the `.quarantine` directory, located at the root of the volume in which the infected file resides. For example, if you scan the infected file `/vol1/dir1/file1.txt`, the virus is logged in `/vol1/.quarantine/virus.log`.

Enabling Antivirus Protection

Follow these steps to enable antivirus protection, referring to [“Configure Antivirus Panel” on page 350](#) for detailed field information.

1. From the navigation panel, choose Antivirus Configuration→ Configure Antivirus.
The Configure Antivirus panel is displayed.
2. Select the Enable Antivirus checkbox.
3. Specify the IP address of the system that is running the scan engine software you want to use. You can specify up to four scan-engine systems.
4. Specify the port on the scan-engine system that the scan engine uses to detect scan requests. This is typically port 1344.
5. Specify the maximum number of file scan operations (connections) that the scan engine can perform simultaneously. The default number is two connections, but is typically set higher.
6. Specify the maximum size of a file that can be sent to the scan engine. Then select the units for the size, either MB or GB.
Note: The maximum size must not exceed the processing potential of the scan engine. Most scan engines have a maximum of 2 GB.
7. Select the action to take when a file exceeds the size limit, either Allow or Deny.
8. Specify the types of files to include and exclude from virus scanning.
9. Click Apply to save your settings.

If you use the Trend Micro’s scan engine, see [“Enabling Trend Micro Antivirus Protection” on page 73](#) to complete the setup procedure.

Excluding Files From Scans

When you enable antivirus protection, you can define that all files of a specific file type are excluded from the virus scan.

You can also specify a volume, a share, or a host to be excluded. To exempt a volume or share, define whether to include it in the virus scan when you create it. To exempt a host’s share, edit the approve file, /dvol/etc/approve, using the following format:

```
vscan sharename host|hostgroup access=noscan
```


For information on exempting an existing volume, see “[Editing File Volume Properties](#)” on page 56.

For information on exempting an existing share, see “[Editing an Existing SMB Share](#)” on page 118

Enabling Trend Micro Antivirus Protection

To use the Trend Micro scan engine, InterScan Web Security Suite (IWSS), with the Sun StorageTek NAS OS software’s ICAP connections, you must use the most recent patch and adjust the IWSS configuration.

If you have not yet installed the IWSS 2.5 software, follow the procedure in “[To Install IWSS 2.5](#)” on page 73

If you have already installed the IWSS 2.5 software, follow the procedure in “[To Install IWSS 2.5 for Windows Patch 2](#)” on page 74

If you have already installed the IWSS 2.5 software with the latest patch and are running in ICAP mode, following the procedure in “[To Configure the IWSS Scan Engine for Sun StorageTek NAS OS](#)” on page 75

▼ To Install IWSS 2.5

1. Go to Trend Micro’s download site: <http://www.trendmicro.com/download>.
2. Navigate to Internet Gateway → InterScan Web Security Suite.
3. Click on `iwss-v25-win-b1334.zip` to download the software.
4. Extract the zip file to a temporary folder.
5. Double-click on `Setup.exe` to start the InstallShield Wizard and configure the software. In addition to setting the attributes for the software’s operation, you will be prompted to enter:
 - A password for the system administration account
 - A password for the IWSS web console
 - If this software will use a proxy server, the IP address and port number of your site’s proxy server
6. At the Welcome screen, click Next.
7. Select `Install IWSS on this machine` and click Next.
8. Click Yes to accept the terms of the license agreement.
9. Verify that the system meets the minimum requirements and click Next.

10. Accept the default installation folder and click Next.
11. Clear the checkboxes for the following attributes and then click Next:
 - FTP Scanning
 - SNMP Notifications
 - Control Manager for IWSS
 - Register With Control Manager
12. In the HTTP Handler panel, select ICAP Server and click Next.
13. In the Database Settings panel, verify that Default (MSDE) is selected and click Next.
14. In the Password field, enter a password for the system administration account, sa, and click Next.
15. In the Notification Handling panel, click Next.
16. In the IWSS Administration Account panel, enter a password for the IWSS web console and click Next.
17. In the Connection Settings panel, set up the proxy server if the system uses one to connect to the Internet. Enter the IP address and port number for the proxy server. Click Next.
18. In the Product Activation panel, enter the activation code of IWSS if it is available. You can enter this code at a later time, using the IWSS web console.
19. In the World Virus Tracking panel, click Next.
20. In the Settings Review panel, review your selections and click Next to continue.
21. Wait while the software is installed. When the process is complete, click Next to reboot the system.

After the system reboots, complete the procedure described in [“To Configure the IWSS Scan Engine for Sun StorageTek NAS OS” on page 75](#)

▼ To Install IWSS 2.5 for Windows Patch 2

1. Go to Trend Micro’s download site: <http://www.trendmicro.com/download>.
2. Navigate to Internet Gateway → InterScan Web Security Suite → Patches.
3. Click on `iwss_25_win_en_patch2.zip` to download the patch.
4. Extract the zip file to a temporary folder.
5. Double-click on `TrendIWSSPatch.exe` to extract the patch.

6. Click on Install to start the installation process.
7. At each message that the installation process cannot stop or start the IWSS-FTP service or the Trend Micro Management Infrastructure service, click Retry to ignore the message.

When the installation is complete, complete the procedure described in [“To Configure the IWSS Scan Engine for Sun StorageTek NAS OS” on page 75](#).

▼ To Configure the IWSS Scan Engine for Sun StorageTek NAS OS

1. Open the IWSS web console. Navigate to Programs → Trend Micro IWSS → IWSS Web UI → Administration Interface. Type the password for the web console and click Enter.
2. Navigate to HTTP → ICAP Settings.
 - a. Select Enable X-Virus-ID ICAP header
 - b. Select Enable X-Infection-Found ICAP header
 - c. Click Save.
3. Open Windows Explorer and navigate to C:\Program Files\Trend Micro\IWSS\ directory.
4. Open the intscan.ini file in a text editor.
 - a. Change the value of “disable_infected_url_block” to “yes.”
 - b. Save and close the file.
5. Restart Trend Micro’s Windows service:
 - a. Choose Settings → > Control Panel → > Administrative Tools → > Services
 - b. In the list of services, right-click Trend Micro InterScan Web Security Suite for HTTP and click Restart.

Server Port Management

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

This chapter includes the following sections:

- [“About Port Locations and Roles” on page 77](#)
- [“About Alias IP Addresses” on page 78](#)
- [“Bonding Ports” on page 79](#)

About Port Locations and Roles

NAS appliances and gateway systems identify ports based on their type, and their physical and logical location on the server. To identify the port locations for your system, refer to the *Getting Started Guide* for your NAS appliance or gateway system.

Each port must have an assigned role, as follows:

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

In cluster configurations, the primary port plays an integral part in the failover process. When you assign this role to a port, the partner server in the cluster saves a copy of the IP address of that port as an inactive alias IP address. In addition, when you configure alias IP address on either server, the partner server holds those IP address as additional inactive alias IP addresses. If a failover occurs, the healthy server activates the inactive alias IP addresses corresponding to the IP addresses for the failed server, allowing network access to continue as if the failed server were still active.

- **Independent** – The port role of Independent identifies an active network port used for purposes other than serving data, such as backup.

In a cluster configuration, the independent port does not participate in the failover process. You cannot bond (aggregate) independent ports or add alias IP addresses to them. You can assign any number of independent port roles, but assign only one per server.

- **Mirror** – The port role of Mirror is applicable only with the Sun StorageTek File Replicator option is licensed and enabled. It indicates that the port connects this server to another server for purposes of mirroring file volumes. Use the same port on both the source and target servers for mirroring. For more information about mirroring, see [“About Mirroring” on page 133](#).
- **Private** – The port role of Private is applicable only for cluster appliances and cluster gateway systems. It is reserved for the heartbeat, a dedicated network link that constantly monitors the status of the other server. Each server in a dual-server configuration has one and only one private port.

About Alias IP Addresses

Internet protocol (IP) aliasing is a networking feature that lets you assign multiple IP addresses to a single port. Typically, aliases specify the IP addresses of obsolete systems that have been replaced by NAS storage.

All of the IP aliases for the selected port must be on the same physical network and share the same *netmask* and *broadcast address* as the first, or primary, IP address specified for the selected port.

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

On cluster appliances and gateway systems, you can only add alias IP addresses to ports that are assigned a primary role. (See [“About Port Locations and Roles” on page 77](#) for a description of port role options.) To ensure a successful failover in the event that one server fails, you must split the alias IP addresses evenly between the servers, assigning no more than four alias IP addresses to the primary port on each server. The other five slots are reserved for use during failover, when the server that remains operational will take over the IP address and (up to four) alias IP addresses from the failed server. This allows network access to continue with minimal interruption. See [“Enabling Server Failover” on page 22](#) for details on head failover.

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

Bonding Ports

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

- [“About Port Bonding” on page 79](#)
- [“About Port Aggregation Bonds” on page 79](#)
- [“About High-Availability Bonds” on page 80](#)
- [“Bonding Ports on a Single-Server System” on page 80](#)
- [“Bonding Ports for Cluster Configurations” on page 81](#)
- [“Example: Dual-Server Port Bonding” on page 83](#)

About Port Bonding

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

NAS appliances and gateway systems support Etherchannel bonding, a subset of the 802.3ad specification. Refer to your switch documentation for Etherchannel bonding before attempting to set up port bonding.

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

About Port Aggregation Bonds

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

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

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

About High-Availability Bonds

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

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

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

Bonding Ports on a Single-Server System

You can bond ports after configuring them. However, alias Internet Protocol (IP) addresses and some other aspects of the original configurations might change. After you create a port bond, see [“About Configuring Network Ports” on page 25](#) to configure the port bond. After you bond two or more ports, you cannot add IP aliases to the individual ports, only to the bond.

To bond ports on a single-server system:

1. From the navigation panel, choose 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. Select at least two available ports to bond by clicking the desired port in the Available NIC Ports field, and then clicking > to add it to the NIC Ports in This Bond list.

If you chose Port Aggregation in [Step 3](#), you must select ports that have the same type of interface and are connected to adjacent ports.

Note: Do not create more than one bond per NIC pair.

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

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

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

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

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

To add alias IP addresses to the port bond, see [“Configuring Network Adapters” on page 25](#).

Bonding Ports for Cluster Configurations

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

You can bond ports after configuring them. However, alias Internet Protocol (IP) addresses and some other aspects of the original configurations might change. After you create a port bond, see [“About Configuring Network Ports” on page 25](#) to configure the port bond.

For more information on dual-server port bonding, see [“Example: Dual-Server Port Bonding” on page 83](#).

Note: You can use only ports with a Primary role for port bonding. For more information about port roles, see [“About Port Locations and Roles” on page 77](#).

To bond ports on a dual-server system:

1. From the navigation panel, choose Network Configuration > Bond NIC Ports.
2. Click Create.
3. From the Available NIC Ports list, select the ports you want to bond. This list includes all ports that are not already part of a port bond.

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

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

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

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

Note: Due to timing issues, it is possible to create multiple bonds with the same ports. Do not attempt to create more than one bond per NIC pair.

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

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

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

6. To add alias IP addresses to the port bond, see [“Configuring Network Adapters” on page 25](#).

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

Example: Dual-Server Port Bonding

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

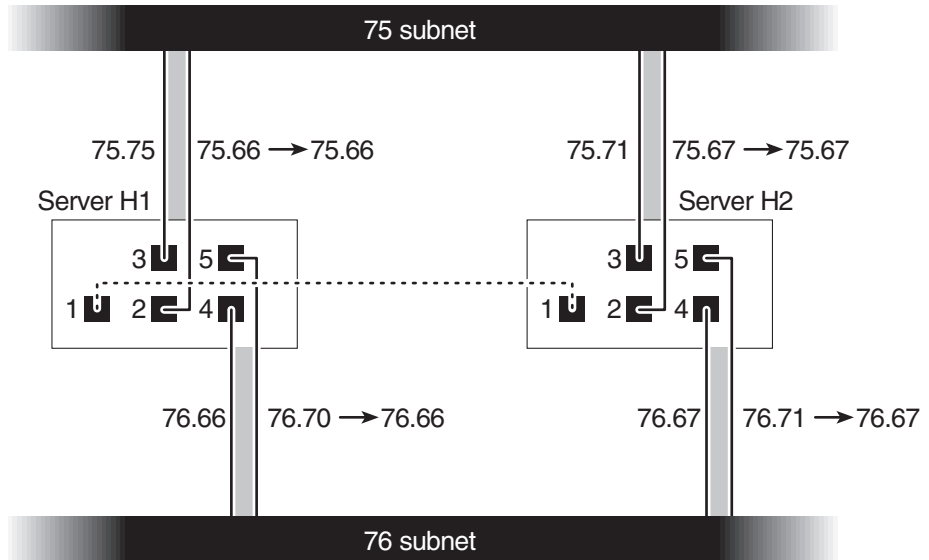


FIGURE 5-1 Dual-Server Port Bonding

TABLE 5-1 lists the Internet protocol (IP) when Ports 2 and 3 are bonded, and Ports 4 and 5 are bonded

TABLE 5-1 Dual-Server Port Bonding Example

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

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

Server	Ports to Be Bonded		Port Bond		
	Name	Primary IP Address	Name	Primary IP Address	Back-Up IP Address
2	Port 2	192.1xx.75.67	Bond 1	192.1xx.75.67	192.1xx.75.66
	Port 3	192.1xx.75.71			
	Port 4	192.1xx.76.67	Bond 2	192.1xx.76.67	192.1xx.76.66
	Port 5	192.1xx.76.71			

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

In the event of head failover, the surviving server activates the IP addresses of the failed server. You can add alias IP addresses to the primary IP address of a port bond and those IP addresses participate in the failover process. For more information about IP aliases, see [“About Alias IP Addresses” on page 78](#).

Active Directory Service and Authentication

This chapter describes Active Directory Service (ADS) in detail, Lightweight Data Access Protocol (LDAP) setup, and how to change name service lookup order. For setup instructions for other name services, refer to [“Managing Name Services” on page 27](#).

This chapter includes the following sections:

- [“About Supported Name Services” on page 85](#)
- [“Using Active Directory Service” on page 86](#)
- [“Setting Up LDAP” on page 91](#)
- [“Changing the Name Service Lookup Order” on page 92](#)

About Supported Name Services

The NAS software supports a variety of name services for both Windows networks and Unix networks. These name services include:

- **ADS** – Active Directory Service (ADS) is a Windows 2000 name service integrated with the Domain Name Service (DNS, see [“Setting Up DNS” on page 30](#)). 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 performs ADS updates. See [“About Active Directory Service” on page 86](#) for more information.
- **LDAP** – Lightweight Data Access Protocol (LDAP) is a Unix service that enables authentication.

- **WINS** – A Windows Internet Naming Service (WINS) server resolves NetBIOS names to Internet Protocol (IP) addresses, allowing computers on your network to locate other NetBIOS devices more quickly and efficiently. The WINS server performs a similar function for Windows environments as a DNS server does for Unix environments. See [“Setting Up WINS” on page 29](#) for more information.
- **DNS** – Domain Name Service (DNS) resolves domain names to IP addresses for the system. This service enables you to identify a server by either its IP address or its name. See [“Setting Up DNS” on page 30](#) for more information.
- **NIS** – Network Information Service (NIS) configures the system to import the NIS database. It administers access to resources based on the users group and host information. See [“Setting Up NIS” on page 31](#) 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 32](#) for more information.

Using Active Directory Service

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

- [“About Active Directory Service” on page 86](#)
- [“Enabling ADS” on page 87](#)
- [“Verifying Name Service Lookup Order” on page 89](#)
- [“Verifying DNS Configuration” on page 89](#)
- [“Publishing Shares in ADS” on page 90](#)
- [“Updating ADS Share Containers” on page 90](#)
- [“Removing Shares From ADS” on page 91](#)

About Active Directory Service

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

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

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

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

Through the graphical user interface, you enable and configure ADS on the [“Configure Domains and Workgroups Panel” on page 452](#). This enables the NAS software to perform ADS updates.

After enabling and configuring ADS on the Configure Domains and Workgroups panel, you can enable ADS to publish Sun StorageTek shares in the ADS directory. To do so, create or update SMB shares on the [“Configure Shares Panel” on page 457](#) and specify the share container for each share that you want to publish.

Setting up ADS involves the following steps:

1. Enabling ADS, as described in [“Enabling ADS” on page 87](#).
2. Verifying name-service order, as described in [“Verifying Name Service Lookup Order” on page 89](#).
3. Verifying that DNS is enabled and configured to support ADS, as described in [“Verifying DNS Configuration” on page 89](#).
4. Publishing shares in ADS, as described in [“Publishing Shares in ADS” on page 90](#).

Enabling ADS

To enable Active Directory Service (ADS):

1. From the navigation panel, choose 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. From the navigation panel, choose Windows Configuration > Configure Domains and Workgroups.

5. Select the Enable ADS checkbox.
6. In Domain, type the Windows 2000 Domain where ADS is running.
The system must belong to this domain.
7. In the User Name field, type 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 specify 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 administrative user, and the same password can be reused. For more information, refer to the Microsoft Support Services web site, Article Q248808.
8. In the Password field, type the Windows 2000 administrative user's password.
9. In the Container field, type 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. Type the path in terms of the user's cn (common name) folder or ou (organizational unit).
For example, if the user resides in a users folder within a parent folder called "accounting," you would type the following:
ou=users,ou=accounting
Do not include the domain name in the path.
10. If the ADS domain uses sites and the ADS domain controller is in different subnet than the client, type the appropriate site name in the Site field. Otherwise, leave the Site field blank. If specified, the Site will be included when selecting a domain controller.
11. In the Kerberos Realm Info section, type the Realm name used to identify ADS.
This is normally the ADS domain or the Domain Name Service (DNS) domain. When you click Apply, this entry is converted to all uppercase letters. If you leave this field blank, the ADS domain name (in uppercase characters) is used as the Kerberos Realm.
12. Leave the Server field blank, if the system can locate the KDC server through DNS. Otherwise, enter the name of the Kerberos KDC server.
13. type the host name of the of the Kerberos KDC server.
You can leave this field blank.

14. Click Apply to save and invoke your changes.

Verifying Name Service Lookup Order

To verify the name service lookup order:

1. From the navigation panel, choose Unix Configuration > Configure Name Services.
2. Verify that the name service lookup order for Domain Name Service (DNS) is enabled by clicking the Hosts Order tab and ensuring that the DNS service is listed in Services Selected box.
If it is not, select DNS service and click the > button.
3. (Optional) Set the name service lookup order to the correct priority, by using the Up and Down buttons in the Services Selected box. This determines the order in which the selected services are scanned.
4. Click Apply to save any changes.

Verifying DNS Configuration

To verify Domain Name Service (DNS) configuration:

1. From the navigation panel, choose 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, type the DNS Domain Name.
This name must be the same as the Active Directory Service (ADS) domain.
4. In the Server field, type the Internet Protocol (IP) address of the DNS server you want the system to use, and then click the Add button to place the server address in the DNS Server List.
You can 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, type the user name of a Windows 2000 user with the administrative rights to perform secure dynamic DNS updates.
You can leave this field blank for non-secure updates if they are allowed by the DNS server.
7. In the DynDNS Password field, type the password of the Dynamic DNS user.
8. Click Apply to save your changes.
If Dynamic DNS is enabled, the system immediately updates DNS with its host name and IP address.

Publishing Shares in ADS

To publish shares in Active Directory Service (ADS):

1. From the navigation panel, click System Manager to view existing volumes.
2. Right-click the file volume or directory you wish to share, then select Sharing > New Share (or Add Share, if no sharing is in effect yet) from the pop-up menu. Select at the volume level to create a root-level share.
Note: Alternatively, choose Windows Configuration > Configure Shares, then specify the file volume and directory names.
3. Type a share name, then fill in the other screen fields, including the location in the ADS directory where the share will be published (known as the *container*).
For more detailed field information, see [“New Share Window” on page 444](#).
4. Click Apply to add the share to the specified container.
Note: The container must already exist for the share to be published in that container. The system does not create container objects in the ADS tree.

Updating ADS Share Containers

To update Active Directory Service (ADS) share containers:

1. From the navigation panel, click System Manager to view existing volumes.
2. Right-click the file volume or directory for which you wish to update the share container.

3. Select Sharing > Edit Share from the pop-up menu to open the Edit Share window.
Note: Alternatively, choose Windows Configuration > Configure Shares, then select the target share and choose Edit.
4. Modify the container to specify the new location in the ADS directory where the share will be published.
5. Click Apply to update the share container.

Removing Shares From ADS

To remove shares from Active Directory Service (ADS):

1. From the navigation panel, click System Manager to view existing volumes.
2. Right-click the file volume or directory for which you wish to remove a share.
3. Select Sharing > Remove Share from the pop-up menu.
Note: Alternatively, choose Windows Configuration > Configure Shares, then select the target share and choose Remove.
4. From the Remove Share window, select the share to remove then click Apply.

Setting Up LDAP

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

Note: In a cluster configuration, LDAP changes made on one server are propagated immediately to the other server.

To enable the LDAP service:

1. From the navigation panel, choose Unix Configuration > Set Up NSSLDAP.
2. To enable LDAP, check the Enable NSSLDAP checkbox.
3. In the Domain field, type the domain name of the LDAP server (for example, foo.com.).
4. In the Password field, specify the password set on the LDAP server.
5. In the Server field, specify the Internet Protocol (IP) address of the LDAP server.

6. In the Proxy field, specify the proxy domain, depending on the server settings.
7. Click Apply to save the settings.

Changing the Name Service Lookup Order

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

Note: In a cluster configuration, NS lookup-order changes made on one server are propagated immediately to the other server.

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

1. From the navigation panel, choose Unix Configuration > Configure Name Services.
2. Click the Users Order tab to select the order of user lookup.
3. Select a service from the Services Not Selected box.
4. Click > to move it to the Services Selected box.
To remove a service from user lookup, select it and click <.
5. Arrange the order of lookup services in the Services Selected box, by selecting each service and clicking the Up or Down buttons to move it up or down.
The service at the top of the list will be used first.
6. Click the Groups Order tab to select the services to be used for group lookup, then follow the same steps described above to arrange the order of lookup services for groups.
7. Click the Netgroup Order tab to select the services to be used for netgroup lookup, then follow the same steps described above to arrange the order of lookup services for netgroups.
8. Click the Hosts Order tab to select the services to be used for hosts lookup, then follow the same steps described above to arrange the order of lookup services for hosts.
9. 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. It includes the following sections:

- [“Managing Local Group Privileges” on page 93](#)
- [“Configuring Hosts” on page 97](#)
- [“Mapping User and Group Credentials” on page 101](#)
- [“Setting File Directory Security” on page 111](#)

Note: To configure Windows security, see [“Configuring Windows Security” on page 28](#).

Managing Local Group Privileges

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

- [“About Local Groups” on page 94](#)
- [“About Configuring Privileges for Local Groups” on page 94](#)
- [“About Ownership Assignment and Groups” on page 95](#)
- [“Adding and Removing Group Members and Configuring Privileges” on page 96](#)
- [“Configuring NT Privileges for Groups” on page 97](#)

About Local Groups

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

Note: Local groups apply only to Common Internet File System (CIFS) networking.

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

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

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

About Configuring Privileges for Local Groups

Privileges provide a secure mechanism to assign task responsibility on a system-wide basis. Each privilege has a well-defined role assigned by the system administrator to a user or a group. On NAS appliances and gateway systems, 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 they would normally not be able to 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 are shown in the following table. 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.

Privilege	User Activity Permitted
Back up files and directories	Perform backups without requiring read access permission on the target files and folders.
Restore files and directories	Restore files without requiring write access permission on the target files and folders.
Take ownership of files and folders	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 the following table. Members of the local administrators group can take ownership of any file or folder and members of the Backup Operators can perform backup and restore operations.

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

About Ownership Assignment and Groups

By default, the Domain Admins group of the domain that the appliance or gateway system is a member of is a member of the local administrators group. Thus, when a member of the Domain Admins (including the domain administrator) creates or

takes ownership of a file or folder, ownership is assigned to the local administrators group. This ensures maximum portability if the system is moved from one domain to another: objects owned by the local administrators group are still accessible to members of the new domain administrator group.

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

On Windows systems, the domain administrator membership of the local administrator group can be revoked. In such cases, members of the domain administrator group are treated as regular users. On NAS appliances or gateway systems, 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 a NAS appliance or gateway system.

Adding and Removing Group Members and Configuring Privileges

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

Note: In a cluster configuration, changes made to user groups on one server are propagated immediately to the other server.

To add a group, do the following:

1. From the navigation panel, choose Windows Configuration > Configure Groups.
2. Click Add Group.
3. In the Group field, type the name of the group.
4. In the Comment field, type a description of or comments about the group.
5. Click Apply to save your changes.

To remove a group, do the following:

1. From the navigation panel, choose Windows Configuration > Configure Groups.
2. Select the group you want to remove.

3. Click Remove Group.
4. Click Apply to save your changes.

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

1. From the navigation panel, choose Windows Configuration > Configure Groups.
2. Highlight the group to which you want to add members, or from which you want to remove members.

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

3. In the Group Members box, highlight the member you want to add or delete, and click the Add or Delete icon.
4. Click Apply to save your changes.

To configure privileges for the group, use the Configure Privileges panel. For more information, see [“Configuring NT Privileges for Groups” on page 97](#).

Configuring NT Privileges for Groups

Follow the steps below to configure NT privileges.

Note: In a cluster configuration, changes made to NT privileges on one server are propagated immediately to the other server.

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

Configuring Hosts

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

- [“About Configuring Hosts” on page 98](#)
- [“Adding and Editing Hosts” on page 98](#)
- [“Adding and Editing Host Groups” on page 100](#)

About Configuring Hosts

The Set Up Local Hosts panel enables you to add, edit, or remove entries from the system host file. The table shows current host information, including host name, host Internet Protocol (IP) address, and whether the host is trusted.



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

Adding and Editing Hosts

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

- [“About Trusted Hosts” on page 98](#)
- [“Adding a Host Manually” on page 98](#)
- [“Editing Host Information” on page 99](#)
- [“Removing a Host Mapping for a Host” on page 99](#)

Note: In a cluster configuration, changes made to the host definitions on one server are propagated immediately to the other server.

About Trusted Hosts

The Set Up Local Hosts panel lets you view and edit host information and designate whether a host is trusted. A `root` user on a Network File System (NFS) client has root privileges on the NAS appliance or gateway system if that client was defined as a trusted host and has access to all files regardless of file permissions.

Adding a Host Manually

Follow these steps to manually add a host to the system configuration:

1. From the navigation panel, choose `Unix Configuration > Configure NFS > Set Up Local Hosts`.

2. Click Add.
3. Type the name by which the host is known on the system.
The host name must begin with an alphabetic character or a number, and can include up to 63 alphanumeric characters, total: a–z, A–Z, 0–9, hyphens (-), and periods (.).
4. Type the Internet Protocol (IP) address of the new host.
5. If necessary, select the checkbox to assign the host Trusted status.
A trusted host has root access to the NAS appliance or gateway system.
6. Click Apply to save your changes.

Editing Host Information

To edit host information:

1. From the navigation panel, choose Unix Configuration > Configure NFS > Set Up Local Hosts.
2. Select the host you want to edit, then click Edit.
3. Revise the host name, Internet Protocol (IP) address, and trusted status information as needed. For detailed information about these fields, see [“Set Up Local Hosts Panel” on page 440](#).
4. Click Apply to save your changes.

Removing a Host Mapping for a Host

To remove a host mapping for a particular host:

1. From the navigation panel, choose Unix Configuration > Configure NFS > Set Up Local Hosts.
2. Select the host that you want to remove by clicking on the entry in the host list.
3. Click Remove.
4. Click Apply.

Adding and Editing Host Groups

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

- [“About Adding and Editing Host Groups” on page 100](#)
- [“Adding a Host Group” on page 100](#)
- [“Adding a Member to a Host Group” on page 101](#)


About Adding and Editing Host Groups

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

- The trusted group – For clients that have root access to the file system, and read and write access to all files and directories in that file system.
- The iso8859 group – For NFS clients that use one of the standardized multilingual single-byte coded (8-bit) graphic character sets defined by ISO 8859, to force translation to a name format that can be stored on the NAS device.
- The euc-kr group – For NFS clients that use the Extended Unix Code (EUC) 8-bit character (Korean) encoding system for file and directory names, to force translation to a name format that can be stored on the NAS device.


Adding a Host Group

To add a host group:

1. From the navigation panel, choose **Unix Configuration > Configure NFS > Set Up Local Hosts**.
2. Click the Add icon () next to the Groups menu to open the Add Hostgroup window.
3. Type the host group name.
The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 80 alphanumeric characters: a-z, A-Z, 0-9, hyphens (-), and periods (.).
4. Click **Apply** to save your changes.

Adding a Member to a Host Group

To add a member to a host group:

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

Mapping User and Group Credentials

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

- [“About Mapping User and Group Credentials” on page 102](#)
- [“About Unix Users and Groups” on page 102](#)
- [“About Windows Users and Groups” on page 103](#)
- [“About Credential Mapping” on page 104](#)
- [“About User Mapping Policies” on page 105](#)
- [“About Group Mapping Policies” on page 106](#)
- [“About Built-In Credential Mapping Policies” on page 108](#)
- [“Mapping Windows Groups and Users to Unix Groups and Users” on page 109](#)
- [“Editing a Mapping Between a Windows Group or User and a Unix Group or User” on page 110](#)

About Mapping User and Group Credentials

NAS servers are designed to reside in a multiprotocol environment and provide an integrated model for sharing data between Windows and Unix systems. Although files can 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 266](#).

Credential mapping is used to establish an equivalence relationship between a Unix user or group defined in a local configuration file or Network Information Service (NIS) database with a Windows domain user or group defined in an Windows Security Accounts Manager (SAM) database. User and group mapping is a mechanism to establish credential equivalence on NAS appliances and gateway systems, to provide common access using either environment.

About Unix Users and Groups

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

About Windows Users and Groups

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

The format of a SID is as follows:

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

TABLE 7-1 shows how to interpret the fields in the SID structure

TABLE 7-1 Fields in the SID

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

For readability, SIDs are often displayed as a string of the form: S-1-5-32-500. This SID contains a version number of 1, the identifier authority is 5 and it contains two subauthorities: 32 and 500. The value 500 is the relative identifier (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. Therefore, a domain user can 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 NAS appliance or gateway system also generates a SID to define its local domain. The SID is generated using an algorithm that produces four subauthorities. The first subauthority has the value 4, which represents a nonunique authority. The other three subauthorities are generated using an algorithm that includes the current time and one of the system's MAC3 addresses to ensure uniqueness. This SID will be used to represent both local and Network Information Service (NIS) users by appending the Unix UID or GID to the domain SID. This SID is stored in the equivalent of a local SAM database.

About Credential Mapping

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

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

The mapping format is as follows:

```
<Unix-username>:<UID>:<Windows-username>:<NTDOMAIN>:<RID>
```

```
<Unix-groupname>:<GID>:<Windows-groupname>:<NTDOMAIN>:<RID>
```

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

```
<username>:<password>:<UID>:<GID>:<comment>:<home directory>:<shell>
```

```
<groupname>:<password>:<GID>:<comma-separated-list-of-usernames>
```

About User Mapping Policies

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

- [“About User Mapping” on page 105](#)
- [“About User Mapping Policy Settings” on page 105](#)
- [“Example: User Mapping Policy” on page 106](#)

About User Mapping

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

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

About User Mapping Policy Settings

There are four user mapping policy settings.

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

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

The appropriate group credentials for the Windows user are obtained using the group mapping algorithm. For details, refer to [“About Group Mapping” on page 106](#).

Example: User Mapping Policy

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

```
john:638:johnm:HOMEBASE:1031
```

```
amw:735:alanw:HOMEBASE:1001
```

About Group Mapping Policies

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

- [“About Group Mapping” on page 106](#)
- [“About Group Mapping Policy Settings” on page 107](#)
- [“Example: Group Mapping Policy” on page 107](#)

About Group Mapping

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

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

About Group Mapping Policy Settings

There are four group mapping policy settings:

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

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

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

Example: Group Mapping Policy

The following example shows a group map that makes the `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
```

About Built-In Credential Mapping Policies

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

- [“About Built-In Credential Mapping” on page 108](#)
- [“Defining the Mapping Policy” on page 108](#)

About Built-In Credential Mapping

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

Defining the Mapping Policy

To define the mapping policy:

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

2. Select a user mapping setting from the Windows <--> Unix User Mapping Choice section. For detailed information about these settings, see [“Configure Mapping Policy Panel” on page 455](#).
3. Select a group mapping setting from the Windows <--> Unix Group Mapping Choice section.
4. Click Apply to save your changes.
For more detail about the interaction between user or group credential mapping and the securable objects within the system, see [“Mapping and Securable Objects” on page 266](#).

Mapping Windows Groups and Users to Unix Groups and Users

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

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

For more information about the interaction between user or group credential mapping and the securable objects within the system, see [“Mapping and Securable Objects” on page 266](#).

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

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

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

The Edit SMB/CIFS Group Map window is displayed.

4. (Optional) In the NT User or the NT Group box, edit the following information:
 - **Account** – Edit the NT account name of the user or group that is currently mapped.
 - **RID** – Edit the relative identifier that uniquely identifies the NT user or group within the NT domain.
5. (Optional) In the Unix User or Unix Group box, edit the following information:
 - **Name** – Edit the Unix user or group name that is currently mapped to the specified NT user or group.
 - **ID** – Edit the identifier that uniquely identifies the Unix user or group within the Unix domain.
6. Click Apply to save your changes.

For more information about the interaction between user or group credential mapping and the securable objects within the system, see [“Mapping and Securable Objects” on page 266](#).

Setting File Directory Security

There are two methods for setting file directory security, described in the following sections:

- [“About Setting File Directory Security in Workgroup Mode” on page 111](#)
- [“Setting File Directory Security in Domain Mode” on page 111](#)

About Setting File Directory Security in Workgroup Mode

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

In Workgroup mode, the system behaves as if no authentication has been performed on the client, and explicitly asks for permission requiring a password with every share-connection request.

See [“Creating Static Shares” on page 116](#) for instructions on setting share-level security while adding a share. See [“Editing an Existing SMB Share” on page 118](#) for instructions on setting share-level security while editing shares.

Setting File Directory Security in Domain Mode

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

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

Note: NAS appliances and gateway systems support security on files and directories only, and setting security on a share will pass that security assignment to the underlying directory.

To set file directory security in Domain mode:

1. Open Windows Explorer.
2. Click Tools > Map Network Drive.
3. In the Map Network Drive window, select a drive letter from the Drive drop-down menu.
4. Locate and select the NAS appliance or gateway system.
5. Click OK.
6. In the Windows Explorer window, right-click the system share for which you want to define user-level permissions.
7. Select Properties from the drop-down menu.
8. Select the Security tab in the Properties window.
9. Click the Permissions button.
10. Set the desired permissions.

See your Windows documentation for more information on setting permissions.

11. Click OK.

Shares, Quotas, and Exports

This chapter describes the various methods of controlling user access to the files and volumes on NAS appliances and gateway systems.

It includes the following sections:

- [“Managing Shares” on page 113](#)
- [“Managing Quotas” on page 121](#)
- [“Setting Up NFS Exports” on page 127](#)

Managing Shares

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

- [“About Shares” on page 114](#)
- [“About Static Shares” on page 114](#)
- [“About Share Access Permissions” on page 115](#)
- [“Configuring Static Shares” on page 116](#)
- [“About Configuring SMB/CIFS Clients” on page 119](#)
- [“About Autohome Shares” on page 119](#)
- [“Enabling Autohome Shares” on page 120](#)

About Shares

Common Internet File System (CIFS) is an enhanced version of the Microsoft Server Message Block (SMB) protocol. SMB/CIFS allows client systems of Windows environments to access files on NAS appliances and gateway systems.

A shared resource, or share, is a local resource on a server that is accessible to Windows clients on the network. On a NAS appliances and gateway systems, 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 users are attached to the server. Autohome shares are temporary shares created when a user logs on to the system and removed when the user logs off.

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

About Static Shares

A static share is created to allow users to map their home directories as network drives on a client workstation. For example, if volume `vol1` contains a home directory named `home` and subdirectories for users `bob` and `sally`, the shares would be defined as shown below:

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

If defining and maintaining a static home directory share for each Windows user who has access to the system is inconvenient, you can use the autohome feature. See [“About Autohome Shares” on page 119](#) for more information.

About Share Access Permissions

When you add a share, you have the option to specify Umask access permissions for the share. The Umask defines the security policy for files and directories created in Share mode. It is a three-digit number that is used to set access permissions when new directories and files are created.

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

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

Note: If the DOS read-only attribute is set in a file create request, all write bits are disabled (“0”) when the Umask option is applied, as shown in [TABLE 8-1](#).

TABLE 8-1 Umask Access Permissions With DOS Read-Only Attribute Set

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

Configuring Static Shares

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

- [“About Configuring Static Shares” on page 116](#)
- [“Creating Static Shares” on page 116](#)
- [“Editing an Existing SMB Share” on page 118](#)
- [“Removing an SMB/CIFS Share” on page 118](#)

About Configuring Static Shares

You can add, view, and update static Microsoft Server Message Block (SMB) shares from two places in the Web Administrator GUI:

- From the Configure Shares panel, by selecting Add or Edit.
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, and umask).
- From the System Manager panel, by selecting a volume or directory and choosing the appropriate option from the right-click menu (Sharing > New Share, Edit Share, or Remove Share; or Add Share).

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

By default, a hidden share is created for the root of each file volume when that volume is created, and is accessible only to Domain Administrators. These shares are typically used by administrators to migrate data and create directory structures. Refer to the Configure Shares screen for these share names.

Creating Static Shares

You must create a file volume before you can create a share. For more information, see [“About Creating a File Volume or a Segment” on page 50](#).

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

1. From the navigation panel, choose Windows Configuration > Configure Shares.

Note: Alternatively, navigate to the target file volume and directory under the System Manager, then right-click and choose the appropriate option from the pop-up menu (for example, Sharing > New Share).

2. Click Add, then fill in the fields as described below.

For more detailed field information, see [“New Share Window” on page 444](#).

3. Type the name of the share you want to add in the Share Name field.
4. (Optional) Add a Comment to describe the share.
5. Select the Mac Extensions Desktop DB Calls checkbox to allow the system to access and set Macintosh desktop database information.
6. Select the volume to share from the Volume Name drop-down menu.
7. If you are sharing at the directory level, type the name of the existing directory. Keep in mind, however, that sharing directories below the volume root eases security administration.

You cannot create a directory in this field. Omit this field to create a root-level share.

8. If you enabled ADS in the Set Up ADS panel, specify the ADS container where the share will be published. See [“Publishing Shares in ADS” on page 90](#) for more information.
9. Type the user ID and group ID, if applicable, as well as the read/write and read-only passwords.

These fields are only applicable if you enable Windows Workgroup mode (not NT Domain mode), as described under [“Configure Domains and Workgroups Panel” on page 452](#). Also refer to [“Configuring Windows Security” on page 28](#) for information about enabling Windows security models.

Windows Workgroup uses share-level security. The User ID (UID) and Group ID (GID) fields in this screen represent the sole means of security for NAS appliance and gateway-system file ownership and access by Windows Workgroup users. In other words, the rights to a directory are determined by the share definition rather than by the user.

You can create multiple shares for the same directory with different UIDs and GIDs. You can also manage individual user and group limitations on the amount of file volume space or number of files used through quotas. For more information about quotas, refer to [“About Managing Quotas” on page 122](#).

10. In the Umask field, specify the file creation mask, if any, you want to apply to this share. This field is available only if Windows Workgroup mode is enabled.
The umask defines the security policy for files and directories created in Share mode. It specifies the permission bits to turn off when a file is created.

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

The following table shows umask to permission examples, including the effect of the DOS read-only attribute. For more information, see [“About Share Access Permissions” on page 115](#).

11. Click Apply to save your changes.

Editing an Existing SMB Share

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

1. From the navigation panel, choose Windows Configuration > Configure Shares.
2. Select the share you want to update, then choose Edit.

Note: Alternatively, navigate to the target file volume and directory under the System Manager, then right-click and choose Sharing > Edit Share from the pop-up menu.

3. Modify the fields you want to change.

For more detailed field information, see [“New Share Window” on page 444](#).

For Edit processing, the share name displays as the Old Share Name field. If you want to change this name, type the new name in the Share Name field.

4. Click Apply to save your changes.

Removing an SMB/CIFS Share

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

1. From the navigation panel, choose Windows Configuration > Configure Shares.
2. Select the share you want to remove from the shares table, then choose Remove.

Note: Alternatively, navigate to the target file volume and directory under the System Manager, then right-click and choose Sharing > Remove Share from the pop-up menu. Select the share to delete and click Apply.

3. From the verifications window, select Yes.

About Configuring SMB/CIFS Clients

After you configure security and network settings, the NAS appliance or gateway system becomes visible to Microsoft Server Message Block (SMB)/Common Internet File System (CIFS) clients by registering with the master browser on its local network. Clients can connect with the NAS storage as follows:

- **Windows 98, XP, and Windows NT 4.0** – Users connect either by mapping the network drive from Windows Explorer, or by clicking the NAS appliance or gateway-system icon in the Network Neighborhood window.

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

- **Windows 2000, XP, and 2003** – If Active Directory Service (ADS) is not installed, users connect either by mapping the network drive from Windows Explorer, or by clicking the NAS appliance or gateway-system icon in the My Network Places window.

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

If ADS is installed, users can connect by clicking on a NAS appliance or gateway-system share published in ADS.

- **DOS** – Users must type the `net use` command to map a share to a drive letter on the command line. They need the UNC path for the NAS appliance or gateway system, which consists of a computer name and share name as follows: `\\computer_name\share_name`.

About Autohome Shares

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

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

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

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

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

Enabling Autohome Shares

When you use the Autohome feature, you must decide under what conditions a temporary share will be allowed to be established. The conditions are set first by any specific rules that you define and then by the default rule that you set, if any.

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

To enable autohome shares:

1. From the navigation panel, choose **Windows Configuration > Configure Autohome**.
2. Select one of the **Default Rules** buttons to set the condition for allowing a share if no specific rule allows a share:
 - Select **No Default Rule** to disallow a share if no specific rule allows one.
 - Select **Use Name Services** to allow a share if the user name is found in either the NIS or NIS+ databases.
 - Select **Use Wildcard** to allow a share with any user name.
3. To create a specific rule:
 - a. Click on the **Add** button to open the **Add/Edit Rule** dialog.

- b. Type the Name of the user account.
- c. Type the user's home directory. Specify the absolute path from the volume name up to the user name or use one of the following substitution characters:
 - Question Mark(?) : substitutes to the first character of the user name
 - Ampersand(&) : substitutes to a whole user name.

Example:

amy /vol1/home/?/ampersand

maps to:

amy /vol1/home/a/amy

For more information on the path, see [“About Autohome Shares” on page 119](#).

- d. Type name of the ADS container if one is installed. For more information, see [“About Active Directory Service” on page 86](#)

- e. Click OK

The new rule is now listed in the Specific Rules section of the Configure Autohome dialog. You can edit the rule by selecting it and clicking on the Edit button. If you create more than one rule, you can change the order of the rules by selecting the Up or Down buttons.

4. Click Apply to save your changes.

Managing Quotas

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

- [“About Managing Quotas” on page 122](#)
- [“Configuring User and Group Quotas” on page 122](#)
- [“Configuring Directory Tree Quotas” on page 125](#)

About Managing Quotas

The Manage Quotas panel enables you to administer quotas on NAS appliance and gateway-system file volumes and directories. User and group quotas determine how much disk space is available to a user or group and how many files a user or group can write to a volume. Directory tree quotas determine how much space is available for a specific directory and/or how many files can be written to it.

See [“About Configuring User and Group Quotas” on page 122](#) to set space and file limits for users and groups. Refer to [“About Configuring Directory Tree Quotas” on page 125](#) to set space and file limits for specific directories.

Configuring User and Group Quotas

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

- [“About Configuring User and Group Quotas” on page 122](#)
- [“Enabling Quotas for a File Volume” on page 123](#)
- [“Adding a User or Group Quota” on page 123](#)
- [“Editing a User or Group Quota” on page 124](#)
- [“Deleting a User or Group Quota” on page 124](#)

About Configuring User and Group Quotas

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

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

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 Limits Grace fields show the amount of time left in the grace periods (blank if you are still within the soft limit).

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

Enabling Quotas for a File Volume

To enable quotas for a file volume:

1. From the navigation panel, choose File Volume Operations > Edit Volume Properties.
2. From the Volumes list, select the file volume for which you are enabling quotas.
3. Select the Enable Quotas box.
4. Click Apply.

Adding a User or Group Quota

To add a user or group quota:

1. From the navigation panel, choose 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 Volume drop-down menu, 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. For detailed information on the disk space limits, see [“Add/Edit Quota Setting Window” on page 363](#).
8. Set limits on the number of files a user or group can write to the file volume. For detailed information on the file limits, see [“Add/Edit Quota Setting Window” on page 363](#).
9. Click Apply to save your changes.

Editing a User or Group Quota

To edit a user or group quota:

1. From the navigation panel, choose 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 Volume drop-down menu, 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. For detailed information on the disk space limits, see [“Add/Edit Quota Setting Window” on page 363](#).
6. Edit the limits on the number of files a user or group can write to the file volume.
7. Click Apply to save your changes.

Deleting a User or Group Quota

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

To delete a user or group quota:

1. From the navigation panel, choose 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, then click Edit.

4. In the Edit Quota Setting window, click the Default option in both the Disk Space Limits and File Limits sections.
5. Click Apply to remove the quota setting.

Configuring Directory Tree Quotas

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

- [“About Configuring Directory Tree Quotas” on page 125](#)
- [“Creating a Directory Tree With a Directory Tree Quota” on page 125](#)
- [“Editing an Existing Directory Tree Quota” on page 126](#)
- [“Deleting a Directory Tree Quota” on page 127](#)

About Configuring Directory Tree Quotas

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

Creating a Directory Tree With a Directory Tree Quota

To create a directory tree with a directory tree quota:

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

6. In the Path field, display the full path of the directory that will contain the new directory that you are creating.

To do this, double-click the folder icon in the box under the Path field. 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. Select whether the quota is reported in megabytes or gigabytes, and type the disk space limit in the Max Value field.

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 type the file limit in the Max Value field.
10. Click Apply to add the quota.

Editing an Existing Directory Tree Quota

To edit an existing directory tree quota:

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

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

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. Type the file limit in the Max Value field.
8. Click Apply to save your changes.

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

Deleting a Directory Tree Quota

To delete a directory tree quota:

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

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

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

Setting Up NFS Exports

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

- [“About Setting Up NFS Exports” on page 128](#)
- [“Creating Exports” on page 128](#)
- [“Editing Exports” on page 129](#)
- [“Removing Exports” on page 130](#)

About Setting Up NFS Exports

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

Any host name beginning with “@” identifies a group of hosts. For example, a host name of @general includes all hosts, and a host name of @trusted includes all trusted hosts. Refer to [“About Configuring Hosts” on page 98](#) for information about trusted hosts.

Creating Exports

You create exports by specifying access privileges for a particular Unix host. To export a file volume only to a set of hosts with root permission (like Sun Solaris or UNIX), use one of the following methods:

- Add the hosts to the trusted group using the Set Up Hosts window.
- Add the set of hosts to a host group and then, in the Configure Export panel’s Map Root User section, select the Root User option to export the file volume against this group.

To create an export:

1. From the navigation panel, choose Unix Configuration > Configure NFS > Configure Exports.

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

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

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

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

6. In the Hosts section, select the host or hosts for which you are defining a Network File System (NFS) export.

Select from the following:

- **Host Netgroups** – To select a netgroup, select this option button. From the drop-down menu, select the netgroup for which you are defining this export.
- **Host Group** – To select a host group, select this option button. From the drop-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 Local Hosts panel, select this option. From the drop-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 Local 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.

Select 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 type the user ID.

8. Click Apply to save the export.

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

Editing Exports

To edit an export:

1. From the navigation panel, choose Unix Configuration > Configure NFS > Configure Exports.
2. Select the export you want to change, and click the Edit button.
3. To change the Access rights, click Read/Write, Read/Only, or No Access.
The Hosts section is read-only.

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

Removing Exports

To remove a Network File System (NFS) export:

1. From the navigation panel, choose Unix Configuration > Configure NFS > Configure Exports.
2. Click the Trash button.
3. Confirm the removal.

System Options

This chapter describes system options you can purchase for the NAS appliance or gateway system:

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

This chapter includes the following discussions:

- [“Activating System Options” on page 131.](#)
- [“About the Sun StorageTek File Replicator Option” on page 132](#)
- [“About the Compliance Archiving Option” on page 147](#)
- [“About the Assured Delete Option” on page 151](#)

Activating System Options

Activating the File Replicator or Compliance Archiving system option requires purchase of one or more licenses. As necessary, contact Sun Services to obtain the required licenses.

To activate an option, specify the license information. In a cluster configuration, you must do this on both servers.

1. From the navigation panel, choose System Operations > Activate Options and click Add to add the license.
2. In the Add License window, type the module name provided by Sun (for example, Sun StorageTek File Replicator).

3. Type 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. Type 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 file volumes can be created. Refer to [“About Compliance Archiving Software” on page 147](#) for more information about the Compliance Archiving software.
5. Type the license key provided by Sun.
6. Click Apply to activate the option.
7. If activating the File Replicator software, enter separate licensing information to the mirrored server, as described under [“Activating File Replicator Software on the Remote Server” on page 137](#).
8. If you have never set the time and date, type 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.

About the Sun StorageTek File Replicator Option

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

- [“About Mirroring” on page 133](#)
- [“About Preparing for Mirroring” on page 134](#)
- [“About Requirements and Limitations for Cluster Configurations” on page 134](#)
- [“Configuring Active and Mirror Servers” on page 135](#)

- “Configuring Mirrored File Volumes” on page 136
- “Avoiding and Correcting a Cracked Mirror” on page 139
- “Setting Warning Thresholds for Mirrored File Volumes” on page 139
- “Breaking the Connection and Promoting a Mirrored File Volume” on page 141
- “Reestablishing Mirror Connections” on page 144
- “Changing Volume Roles” on page 146

About Mirroring

The File Replicator option provides for remote asynchronous replication of file systems, sometimes referred to as *mirroring*:

- Remote - The mirror copy is not located with the original file volume.
- Asynchronous - The local and remote copies do not need to occur at exactly the same time, although they are coordinated.
- Replication - The data is duplicated.
- File system - The level at which data is mirrored.

When mirroring is configured, you can duplicate any or all of the file volumes from one appliance or gateway system onto another. You control which volumes are mirrored. The source server is called the “active server” and the target server is called the “mirror server.”

If the active server fails, you can break the mirror on the mirror server, and then make the mirrored file volume available for users, switching from the active server to the mirror server. This operation is called promoting a mirror volume.

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, but because the processing is transaction-oriented, the integrity of the mirror file system is guaranteed, even during network interruptions or system outages.

File volumes on the mirror server have a partition type of NBD (Network Block Device), which identifies the software module that provides the network transport for file replication. If a mirror file volume is promoted, its partition type is SFS2 (Server File System version 2, a proprietary NAS file system), or SFS2EXT for a segment, like all other file volumes.

When checkpoints are created on the active server, the checkpoints get copied to the mirror server. This can be useful for scheduled backups, or to provide a read-only checkpoint to specific users or applications.

About Preparing for Mirroring

Before you begin mirroring, review the following system requirements:

- Two servers are required for mirroring. The servers can be any model and they can be different models from one another.
- The mirror server must contain an equal or larger amount of storage space than the file volumes to be mirrored.
- The active server and the mirror server must have a reliable, continuously available network connection between them with sufficient capacity. The interface type can be 100 megabit Ethernet or 1000 megabit Ethernet. The servers can be connected through a switch or router. If you are connecting the servers to a router, 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 greater than 1 gigabyte.
- Review the names of the file volume on the active server. After a file volume is mirrored, it cannot be renamed.

About Requirements and Limitations for Cluster Configurations

The following requirements and limitations apply with the Sun StorageTek File Replicator software, when you are mirroring in a cluster configuration.



Caution: When the cluster is in failover mode (that is, one server is in the ALONE state and the other server is in the QUIET state) or any degraded state, do not perform any mirror management operations. Bring the cluster to the NORMAL state before doing any of the mirror management operations.

- Both servers in the cluster configuration must have the Sun StorageTek File Replicator license enabled.
- For any mirror management operations (including New Mirror creation, Change Role, Promote, and Break), both servers in the cluster must be in the NORMAL state.

- Existing mirrors will continue mirroring, even when the cluster configuration fails over. Also, the existing mirrors will continue mirroring when the cluster is restored after a failover.
- Mirror buffering restrictions apply, as described in [“About Mirroring the Mirror Buffer” on page 136](#).

Configuring Active and Mirror Servers

When setting up your systems, designate the roles of the ports connecting the mirroring servers to one another. Then configure mirroring on the active and mirror servers using the Web Administrator interface (see [“About Mirroring the Mirror Buffer” on page 136](#)). Configure each system independently.

To configure the dedicated network ports:

1. From the navigation panel of the active server, choose Network Configuration > Configure TCP/IP > Configure Network Adapters.
2. If you have not done so already, assign the Internet Protocol (IP) addresses and a port role of Primary for the ports that are connected to a local network or subnet.
The active and mirror systems' ports can be on different local subnets. For more information about configuring Transmission Control Protocol/Internet Protocol (TCP/IP), see [“About Configuring Network Ports” on page 25](#).
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, 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 servers are not connected on the same subnet, you must set up a static route between them, using the command-line interface.

This enables the servers to communicate with each other over networks that are not directly connected to their local interfaces. For more information about completing this process, see [“Managing Routes” on page 249](#).

6. Click Apply to save changes.

Configuring Mirrored File Volumes

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

- [“About Mirroring the Mirror Buffer” on page 136](#)
- [“Activating File Replicator Software on the Remote Server” on page 137](#)
- [“Adding a File Volume Mirror” on page 137](#)
- [“Editing a Mirror” on page 138](#)

About Mirroring the Mirror Buffer

Mirroring is performed on a per-volume basis. You can mirror some or all of your file volumes.

Note: File volumes must be greater than 1 gigabyte, a minimum of 1046 megabytes, to be mirrored. A file volume of exactly 1 gigabyte (1024MB) does not have enough available capacity to enable mirroring.

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, create a mirror buffer that is approximately 10 percent of the size of the file volume you are mirroring. The size you specify depends 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, create a mirror buffer that is approximately 25 to 30 percent of the size of the file volume you are mirroring.

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

Activating File Replicator Software on the Remote Server

After you have activated the Sun StorageTek File Replicator option (see [“Activating System Options” on page 131](#)), you must also activate the option on the remote server that contains file volumes you want to mirror.

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

1. Log in to Web Administrator on the server containing the file volumes you want to mirror.
2. In the Add License window, type the module name provided by Sun (Sun StorageTek File Replicator).
3. Type the origination date provided by Sun, using 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. Type the expiration date provided by Sun, using the format *yyyymmdd*.
This is the date through which the license is valid. The date 00000000 means that the license never expires.
5. Type the license key provided by Sun.
6. Click Apply to activate the Sun StorageTek File Replicator.

Adding a File Volume Mirror

To add a file-volume mirror to the configuration:

1. From the navigation panel, choose File Replicator > Manage Mirrors.
2. Click Add.
3. From the Volume drop-down menu, select the file volume to be mirrored.
The file volume to be mirrored must be larger than 1 gigabyte.
4. Type the name of the mirror server in the Mirror Host field.
5. Type the Internet Protocol (IP) address of the mirror server.
This must be the IP address defined for the mirroring network interface card (NIC) on the mirror server.
6. (Optional) Type the alternate IP address for the mirror server.

In the event that the first IP address becomes unavailable, the mirror will be accessed through the alternate IP address.

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

It is a good idea to protect your servers with passwords.

8. Type the size (in megabytes) allocated for file volume's mirror buffer.

This reduces the file volume's free space on the active server by the size specified.

9. Click Apply to create the mirror for the file volume.

During this process, there can be no I/O activity to the mirror volume. The volume is taken offline to avoid transient file system errors and inconsistencies while the mirror is being created.

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 when the mirror reaches In Sync status.

Editing a Mirror

You can add to some of the properties of a mirror file volume that is not in the In Sync state. You cannot change the values that were specified when the mirror file volume was created. You can only specify information that was not specified when the mirror file volume was created. For example, you can add a password if no password was set, but you cannot modify a password.

To edit a mirror:

1. From the navigation panel, choose File Replicator > Manage Mirrors.
2. Select the mirror that you want to edit from the table. It must not be in the In Sync state.
3. Click Edit.
4. Add the alternate IP address, if this field is empty.
5. Add the administrator password required for accessing the mirror host server, if this field is empty.
6. Click Apply to save your changes.

Avoiding and Correcting a Cracked Mirror

If the connection between the two servers is down for some time, or the mirror buffer is too small to handle the number of writes to the master file volume, the mirror might show signs of *cracking*. You can recognize this when the mirror begins replicating again, and the Sync Status on the File Replicator > Manage Mirrors panel is no longer In Sync.

The mirror file volume will go off-line until the replication is finished. View the Sync Status field in the Manage Mirrors panel to view the replication percentage completed (Initializing Mirror Buffer *percent-complete*).

If the replication completes successfully, the mirror did not crack. Take these precautionary steps to minimize the possibility that the mirror will crack in the future:

1. Establish a faster network connection between the two servers.
2. Periodically, quiesce or reduce the I/O activity to the active file system, and allow the mirror to reach the In Sync state.

If the replication cannot complete (typically because the original server died, or a logical unit number (LUN) was lost), the mirror is cracked. Contact Sun Services to step through the process of rebuilding the mirror.

Setting Warning Thresholds for Mirrored File Volumes

This section provides information about setting warning thresholds. The following subsections are included:

- [“About Setting Warning Thresholds” on page 140](#)
- [“Setting Up the Threshold Alert” on page 140](#)

About Setting Warning Thresholds

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

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

There can be no I/O activity to the mirror volume during the resync. The volume is taken offline to avoid transient file system errors and inconsistencies.

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

Setting Up the Threshold Alert

To set up the threshold alert:

1. From the navigation panel, choose 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 issued.
3. Select the Mirroring Buffer Threshold 2.

This is the percentage of mirror buffer usage that triggers the second alert. The default value is 80 percent.
4. Select the Mirroring Buffer Threshold 3.

This is the percentage of mirror buffer usage that triggers the third alert. The default value is 90 percent.
5. Select the Alert Reset Interval (Hours).

This is the amount of time the system waits before re-issuing an alert if the condition re-occurs within the interval.

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

The default value for this field is 24 hours.

6. Click Apply to save your changes.

Breaking the Connection and Promoting a Mirrored File Volume

To promote a file volume on the mirror server, you must first break the mirror connection. This section describes how to break the connection and promote a file volume. It contains these discussions:

- [“Breaking the Connection Between Mirror Servers” on page 141](#)
- [“Promoting a Mirrored File Volume” on page 142](#)
- [“Promoting iSCSI LUNs” on page 143](#)

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 down and you cannot access it to break the connection, you can break the mirror connection from the mirror server instead.

To break a mirror connection between mirror servers:

1. From the navigation panel of the active server, choose 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. After 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 142](#).

Promoting a Mirrored File Volume

If 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. After a mirror connection is broken and the mirrored file volume promoted, the original and mirrored file volumes are completely independent.

Note: There is no difference between promoting a compliance-enabled file volume and a non-compliance-enabled volume. The processing is identical.

Note: If the file volume being promoted contains iSCSI logical unit numbers (LUNs), you must promote each iSCSI LUN after promoting the file volume itself.

To promote a file volume on the mirror server, you must first break the mirror connection. See [“Breaking the Connection and Promoting a Mirrored File Volume” on page 141](#) for instructions. Then:

1. From the navigation panel of the mirror server, choose File Replicator > Manage Mirrors.
2. Click Promote.
3. In the Promote Volume window, select the file volume to promote.
4. (Optional) To change the name of the promoted file volume, specify the new name for the volume at the bottom of the window.

This feature is particularly useful for compliance-enabled file volumes, which can be renamed only at the time of promotion. Volumes that are not mirrored (in other words, that are not compliance-enabled) can be renamed at any time.

Unless you rename a compliance-enabled file volume when you promote it, you cannot mirror that volume back onto the original active server, because the original file (by the same name) will already be on that server.

5. Click Apply.

It might take several minutes to complete this process. A status message is displayed when the process is complete. For the mirrored file volume to be promoted, 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 promotion process.

After you promote the file volume, you might need to reconfigure access rights. Microsoft Server Message Block (SMB) share information is carried over, but you must configure any Network File System (NFS) file volume access and NFS exports for this file volume again. For more information on setting up NFS exports, see [“About Setting Up NFS Exports” on page 128](#).

6. If the promoted file volume contains iSCSI LUNs, promote each iSCSI LUN after completing the file-volume promotion (above).

Promoting iSCSI LUNs

After promoting a file volume that contains iSCSI logical unit numbers (LUNs), you must promote each iSCSI LUN on that file volume. To do this:

1. Define the access list for each iSCSI LUN you want to promote, referring to [“Creating an iSCSI Access List” on page 62](#) for instructions.
2. From the navigation panel, choose iSCSI Configuration > Configure iSCSI LUN.
3. Click Promote iSCSI LUN.
4. In the Promote iSCSI LUN panel, specify the iSCSI target IQN identifier for the LUN to be promoted (Name field), the name of the file volume where the promoted LUN resides (that is, the name of the file volume as it was promoted), and the access list used for the LUN. Refer to [“Promote iSCSI LUN Window” on page 386](#) for further details.

The Alias field is filled in according to the original iSCSI LUN definition, but you can edit it.

5. Each iSCSI LUN must only be advertised once on the network. After promoting the iSCSI LUN, therefore, make sure its iSCSI Qualified Name (IQN) is only visible from the promoted-to volume.
6. Click Apply to promote the iSCSI LUN.

Reestablishing Mirror Connections

This section provides information about reestablishing mirror connections. The following subsections are included:

- [“Reestablishing a Mirror Connection” on page 144](#)
- [“Breaking the Mirror Connection on the Active Server” on page 145](#)
- [“Deleting the Out-of-Date File Volume From Server 1” on page 145](#)
- [“Mirroring the Up-to-Date File Volume From Server 2 to Server 1” on page 145](#)

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 brings the mirror back to an In Sync state when it comes back online.

In the examples that follow, Server 1 is the original active server that failed and contains the out-of-date volume, and Server 2 is the original mirror server that now contains the up-to-date volume.

Reestablishing a mirror connection entails the following steps:

1. Make sure the mirror on Server 1 is broken, referring to [“Breaking the Mirror Connection on the Active Server” on page 145](#).
2. Delete the out-of-date file volume on Server 1, as detailed under [“Deleting the Out-of-Date File Volume From Server 1” on page 145](#).
3. Mirror the up-to-date file volume from Server 2 back to Server 1, described under [“Mirroring the Up-to-Date File Volume From Server 2 to Server 1” on page 145](#).
4. Change the role on Server 2 (see [“Changing Volume Roles” on page 146](#)).

This makes Server 1 active, and Server 2 the mirroring target.

Breaking the Mirror Connection on the Active Server

To break the mirror connection on the active server:

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

Deleting the Out-of-Date File Volume From Server 1

After a file volume on the mirror server is promoted, it becomes the current version of the file volume. The file volume on the active server is out of date and must be deleted, as follows:

1. From the navigation panel of Server 1, choose File Volume Operations > Delete File Volumes.
2. Select the file volume that was being mirrored (and is now out of date).



Caution: Before completing the following step, make sure you selected the out-of-date file volume on the active server. Also make sure that the up-to-date file volume on the mirror server has been verified and promoted.

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

Mirroring the Up-to-Date File Volume From Server 2 to Server 1

To mirror the up-to-date file volume from Server 2 to Server 1:

1. Open a web browser window to Server 2.
2. From the navigation panel, choose File Replicator > Manage Mirrors.
3. Click Add.
4. From the Volume drop-down menu., select the file volume to be mirrored
5. Type the mirroring name of Server 1 in the Mirror Host field.

6. Type the Internet Protocol (IP) address of the Server 1 port used for the mirroring connection.
7. Type the alternate IP address.
8. If you need an administrative password to access Server 1, type it in the Password field.
If there is no administrative password, leave this field blank.
9. Type the size of the mirror buffer.
For more information about the mirror buffer, see [“About Mirroring” on page 133](#), and [“About Mirroring the Mirror Buffer” on page 136](#)
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.
There can be no I/O activity to the mirror volume during synchronization. The volume is taken offline to avoid transient file system errors and inconsistencies while the mirror is being created.
11. In the Manage Mirrors panel on Server 1, select the promoted file volume then click Change Roles.
See [“Changing Volume Roles” on page 146](#) for more information.
You have reestablished the original mirroring connection.

Changing Volume Roles

An administrator can switch roles between an active file 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: Make sure the file volumes are in sync before changing roles.

You can request the change in roles from the active or mirror server. To do this:

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

About the Compliance Archiving Option

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

- [“About Compliance Archiving Software” on page 147](#)
- [“About Enabling Compliance Archiving” on page 148](#)
- [“About Compliance With Mandatory Enforcement” on page 148](#)
- [“About Compliance With Advisory Enforcement” on page 149](#)
- [“About Compliance Auditing” on page 149](#)

About Compliance Archiving Software

The Compliance Archiving software helps a company address business practices and regulatory compliance rulings regarding the retention and protection of information. Such rulings and frameworks for records retention and protection include the Security and Exchange (SEC) Regulation 17 CFR § 240.17a-4 (17a-4), Sarbanes Oxley Act, BASEL II, and numerous data protection and privacy directives.

The Compliance Archiving software was designed 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.

Note: Gateway configurations support compliance with advisory enforcement but not mandatory enforcement.

Note: Compliance archiving (WORM storage) is not supported on iSCSI LUNs.

To ensure the strongest possible enforcement of your data retention policies, it is essential that you provide for the physical security of your NAS device. Software-controlled data retention is no stronger than the physical safeguards used to control access to the system’s hardware.

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 194](#).

About Enabling Compliance Archiving

The Compliance Archiving software enforces compliance archiving guidelines for data retention and protection, on NAS appliances and gateway systems. Compliance archiving can be enforced in both a less stringent form (referred to as “advisory enforcement”) and in a stringent form (referred to as “mandatory enforcement”).

You enable the enforcement of compliance archiving guidelines separately for each file volume, and you must do so when the file volumes is initially created. Follow the instructions under [“Creating a File Volume or Segment Using the Create File Volumes Panel”](#) on page 51 to create a compliance-enabled volume.



Caution: Do not enable compliance archiving on file volumes that will be used by applications and users that are not aware of the different data retention rules enforced by the Compliance Archiving software.

When enabling the Compliance Archiving software, be sure that the NAS server’s system clock and the client system’s server clock are synchronized. You can synchronize the NAS server to an external time source using NTP, as described in [“About Time Synchronization”](#) on page 68. A time difference between a client and the NAS server could cause the server to apply the default retention period when a client requests a retention time shorter than the clock skew.

For Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems, proper operation of the Compliance Archiving software requires the correct physical configuration of the NAS appliance hardware. In particular, the redundant array of independent disks (RAID) controller must not be connected to any device or network, other than a private Fibre Channel connection to the NAS server, and (for non-gateway configurations), connections to any expansion units. There are no such requirements for Sun StorageTek 5210 NAS appliances.

About Compliance With Mandatory Enforcement

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

- You cannot destroy a compliance file volume with mandatory enforcement.
- You cannot destroy a WORM file until the retention period has been met.

- You can increase or decrease the default retention period of a file volume, but you can only increase the retention period of a WORM file.

Note: Gateway configurations do not support compliance with mandatory enforcement.



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

About Compliance With Advisory Enforcement

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

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

Note: Before deleting a file volume, copy the audit logs for that volume to a different file system; otherwise, those logs will be lost.

- An authorized administrator can increase and decrease retention time.
- Default retention time when shipped from the factory is zero days and can be changed.

Note: Decreasing the retention time and removing retained files before the retention period has expired must be performed by the root user from a trusted host. See [See “Managing Trusted Hosts” on page 269.](#)

When a compliance-enabled file 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: Changing a compliance-enabled file volume with advisory enforcement to mandatory enforcement is not supported for gateway configurations.

About Compliance Auditing

Compliance auditing provides a text-based log for attempted efforts to modify or delete data (with or without proper authority) and is enabled through the use of the Data Retention Audit Service (DRAS) API, which includes the following features:

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

The set of 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

Note: A request to write to a retained file might not be written to the audit log. This can occur if you use an application that attempts to determine the access permissions before writing to a file. The application does not issue a write request if write permission is not available for a retained file.

The audit logs for each compliance-enabled file volume reside in a hidden directory called `.audit$` in that volume's root directory. The audit log must be accessed by a root user from a trusted host, or by a Windows domain administrator if you are running CIFS in domain mode. See ["Managing Trusted Hosts" on page 269](#) for more information.

Audit log records are text-based and can be accessed through network protocols, including Network File System (NFS) and Common Internet File System (CIFS). The `.audit$` directory must be included in the share path for the contents to be viewed by clients running Windows 2000 or XP. Refer to ["About Shares" on page 114](#) for details about creating shares.

The following table describes the fields in the audit log.

TABLE 9-1 Audit Log Format

Field	Length	Description
Version	7	Data Retention Audit Service version number.
Serial Number	11	Unique sequence number.
Length	5	Length of the audit record.
Timestamp	21	Date and time at which the event occurred.

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

Field	Length	Description
TID	11	Thread ID of the thread from which the event was executed.
Volume ID	11	Volume ID of the file volume on which the audit was performed.
Protocol	9	Network protocol through which the operation was requested.
Inode	11	File-system inode number of the file.
Client IP Address	16	Internet Protocol (IP) address of the client from which the operation was requested.
Server IP Address	16	IP address through which the client request was received.
UID	11	User credentials.
GID	11	Primary group credentials.
Operation	8	Audit event.
Status	variable	Result of the operation.
Domain	variable	Windows domain that the user belongs to, if available.
File/Directory Name	variable	File or directory on which the operation was performed, if available.
Path/Extra Data	variable	Extra information from the audit, if available.

Compliance file 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 file volume falls below this limit, auditable operations will not be executed. A message will be logged indicating that there is not enough space to execute both the operation and the audit, and a warning email will be sent, if email has been configured on the system.

About the Assured Delete Option

This section provides information about the Assured Delete option. The following subsections are included:

- [“About Assured Delete” on page 152](#)
- [“Enabling Assured Delete” on page 152](#)

- [“About Restrictions for Assured Delete” on page 153](#)

About Assured Delete

The Assured Delete feature, also referred to as *data shredding*, *secure delete*, or *true delete*, provides a secure way of deleting data. When it is enabled, files that are removed cannot be recovered by searching through the storage on the disks.

In volumes without the Assured Delete feature, deleting a file does not actually remove any data. Instead, deleting a file only unlinks the file from its parent directory. The file system then reuses the pages when needed. The data on those pages remains on the disk until overwritten when the pages are reused. Until this occurs, sensitive data can be recovered with efforts such as examination of the disks.

When a system is configured to use Assured Delete, deleting a file causes the file system to first overwrite the file’s data pages several times with data patterns before unlinking them from the parent directory. The data pages are released for reuse but no longer contain the original data.

The Assured Delete feature can be configured for any volume except for system volumes. When it is enabled, a hidden directory is created called the shredder. When a user deletes a file from that volume, the file is placed in the shredder and the data blocks for the file are overwritten a specified number of times. When the overwrite operations are complete, the file is moved to the attic directory where it is then unlinked and the data pages can be reclaimed for use by the file system.

The number of times the data blocks are overwritten can be specified, from the default of three times to the maximum of seven times. The data patterns used in the overwrite operation are the following: first pass is 0x00, the last is 0x55, and all passes between the first and last are random patterns.

Enabling Assured Delete

To enable Assured Delete for a volume, use the following command:

```
> fsctl shredding enable <volume>
```

where <volume> is the name of a volume.

To change the number of overwrite operations from the default of three overwrite operations, use the following command:

```
> fsctl shredding enable n <volume>
```


where n is the number of operations, from 3 to 7.

To view the status of shredding operation, use the following command:

```
> fsctl shredding status <volume>
```

The status subcommand displays whether Assured Delete is enabled for the volume, and if so, the number of overwrite operations performed on shredded files. Also, the status subcommand displays the current number of files in the shredder directory for the specified volume.

To disable the Assured Delete feature for a volume, make sure the shredder directory is empty and then use the following command:

```
> fsctl shredding disable <volume>
```

About Restrictions for Assured Delete

The use of the Assured Delete feature has the following restrictions and effects on other functions:

- Do not maintain checkpoints on volumes for which Assured Delete is enabled. Existing checkpointed versions of shredded files cannot themselves be shredded.
- If checkpoints are enabled on a volume, any data blocks that have not already been copied to a checkpoint (data blocks that point to the original file) are not copied and will contain overwritten data (ultimately, all 0x55). These files will appear to be corrupt or to contain nonsense data.
- When Assured Delete is enabled on a volume, the attic directory cannot be disabled.
- When Assured Delete is enabled on a volume, performance is affected. After each overwrite operation, the cache for the entire LUN is flushed to make sure that pages are not replaced in the cache before they are written to dis.
- When Assured Delete is enabled on a compliance volume, the attempts to remove files are recorded in the audit log as "shred" attempts instead of "remove" attempts.
- The shredder directory must be empty before the function can be disabled or before the system OS can be downgraded to a version earlier than 4.21. Disabling the feature or downgrading the OS will not succeed if the directory is not empty.

Monitoring the System

This chapter describes the monitoring functions available for use with NAS appliances and gateway systems. System monitoring is closely related to maintenance functions and many of the monitoring functions described here refer to other chapters where action can be taken to alleviate issues shown by the monitoring functions. The monitoring functions also show the completion or status of management or maintenance activities.

This chapter includes the following sections:

- [“SNMP Monitoring” on page 155](#)
- [“Viewing System Status” on page 157](#)
- [“System Logging” on page 157](#)
- [“System Auditing” on page 160](#)
- [“Viewing Environmental Status” on page 162](#)
- [“Viewing Usage Information” on page 165](#)
- [“Viewing Network Routes” on page 166](#)
- [“Monitoring System Status” on page 167](#)

SNMP Monitoring

This section provides information about Simple Network Management Protocol (SNMP) monitoring. The following subsections are included:

- [“About SNMP Monitoring” on page 156](#)
- [“Setting Up SNMP” on page 156](#)

About SNMP Monitoring

You can conduct Simple Network Management Protocol (SNMP) monitoring by enabling SNMP communications. NAS appliances and gateway systems support SNMP monitoring only (not SNMP management).

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

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

Setting Up SNMP

To set up Simple Network Management Protocol (SNMP):

1. From the navigation panel, choose Monitoring and Notification > Configure SNMP.
2. Select the Enable SNMP checkbox to enable SNMP.
3. Type the SNMP community to which the NAS appliance or gateway system belongs in the Server SNMP Community field.
4. In the Contact Info field, type the name of the person who is responsible for this system.
5. In the System Location field, type the network location.
This location can be physical or logical.
6. To add a new target address, type the following information in an empty row of the SNMP table:
 - **Destination IP Address** – TCP/IP address for the server you want to designate as an SNMP trap destination in the event of system errors.
 - **Port #** – Port to which the system sends traps. The default value is port 162.
 - **Version** – SNMP version (either 1 or 2) from the drop-down menu.
 - **Community** – String for the trap destination.

- **Enable** – Select this checkbox in to enable this target address to become a trap destination.
7. To remove a target address at any time, select the line you want to remove and click the Remove button.
 8. Click Apply to save your changes.

Viewing System Status

The Web Administrator graphical user interface displays basic system status when you first access it. The status screens vary, depending on the functions and physical characteristics of the model. The information is helpful when calling Sun Services, and can provide the first indication of what has failed.

To view system status, click the Home button in the toolbar. [TABLE 10-1](#) describes the information in the system status.

TABLE 10-1 System Status Display

Name	Description
Name	Server name.
Model	System model.
Serial #	Unique serial number of the system.
Up Time	Amount of time elapsed since the system was last turned on.
CPU Load	Current and peak processor load.
OS Version	Current version of NAS software running on the server.
Web Administrator Version	Version of Web Administrator installed on the system.
Head Status	State of server H1 (Cluster only): NORMAL, QUIET, ALONE.
Partner Status	State of server H2 (Cluster only): NORMAL, QUIET, ALONE.
Features Enabled	Any optional features enabled on the system.

System Logging

This section provides information about system logging. The following subsections are included:

- [“About System Logging” on page 158](#)
- [“About System Events” on page 159](#)
- [“Viewing the System Log” on page 160](#)

About System Logging

The system log provides basic information in regard to all system events. The log provides essential information when you are trying to determine what errors occurred and when.



Caution: You must enable remote logging or create a log file on local disk to prevent the log from disappearing on system shutdown. (See [“Setting Up Logging” on page 35](#).) 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 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) might take up to 30 seconds to appear on the event log. If there are multiple changes within that time frame, some events might not be reported.

The following graphic depicts the Display System Log panel.

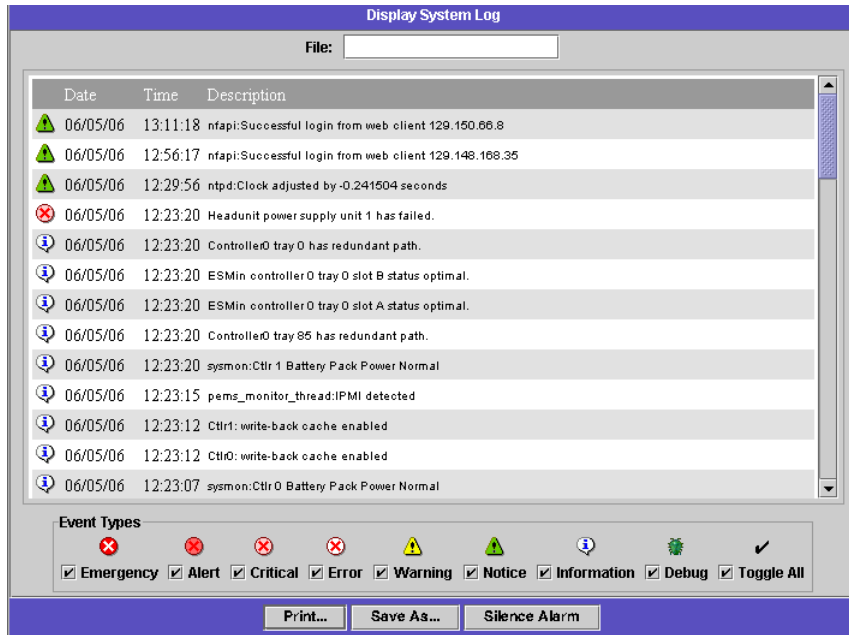


FIGURE 10-1 Display System Log Panel

About System Events

The system log logs eight types of system events, each representing a different priority, or severity level. Each event is represented by an icon, shown in [TABLE 10-2](#).

TABLE 10-2 System Event Icons









Icon	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.

TABLE 10-2 System Event Icons (*Continued*)

Icon	Description
	Error – Specifies any messages that represent error conditions, such as an unsuccessful disk write.
	Warning – Specifies any messages for abnormal, but recoverable, conditions.
	Notice – Specifies important informational messages. Messages without a priority designation are mapped into this priority message.
	Information – Specifies informational messages. These messages are useful in analyzing the system.
	Debug – Specifies debugging messages.

Viewing the System Log

To view the system log:

1. From the navigation panel, choose Monitoring and Notification > View System Events > Display System Log.
2. Check all Event Types you want to view.
See [“About System Events” on page 159](#) for more information.
3. Click Refresh.

Note: If your system log contains error messages stating “Unowned SFS2” volumes, call Sun Services for assistance.

System Auditing

This section provides information about system auditing. The following subsections are included:

- [“About System Auditing” on page 161](#)
- [“About Audit Log Files” on page 161](#)
- [“Setting Up System Auditing” on page 162](#)

About System Auditing

System auditing allows the system administrator to audit particular system events by storing records of those events in audit log files. These log files are stored in binary format on the local file system.

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.

Note: Auditing is separate from `syslog`.

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

About Audit Log Files

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

Log file names are formatted using a date/timestamp, as well as the system host name: `YYYYMMDDhhmmss.not_terminated.host-name`. The timestamps use Greenwich Mean Time (GMT).

For example, if the current log file was started on April 21, 2006 at 1:15 p.m. GMT on an appliance with the host name `a testhost`, the log file would be identified as:

```
20060421131500.not_terminated.testhost.
```

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

After a log file is closed (because it reached its maximum size), the name is converted using the same timestamp format. For example, if the same log file in the above example reached its maximum size on October 30, 2006 at 7:35 p.m. GMT, the name would convert to `20061021131500.20051030193500.testhost.`

Audit log files are assigned zero permissions, and 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, as necessary (and with caution).

To access (read) an audit log, use the `praudit` CLI command, which converts the binary information in the audit logs into readable text. There is no graphical user interface support for reading or removing audit logs.

Setting Up System Auditing

To set up system auditing:

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

Selectable volumes are non-system volumes. You must create special purpose audit volumes. (For instructions, see [“Creating a File Volume or Segment Using the Create File Volumes Panel”](#) on page 51.)

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

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

5. Click Apply to save your settings.

Viewing Environmental Status

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

- [“Viewing Fan Status”](#) on page 163
- [“Viewing Temperature Status”](#) on page 163
- [“Viewing Power Supply Status”](#) on page 163
- [“Viewing Voltage Status”](#) on page 164

Viewing Fan Status

To view the operational status and revolutions per minute (RPM) of all the fans in the appliance or gateway-system server, choose Monitoring and Notification > View Environmental Status > View Fan Status from the navigation panel.

The View Fan Status panel shows the current status of each fan. A green diamond in the Status column indicates that the fan RPMs are normal. A red diamond indicates that the RPMs have exceeded the acceptable range. If the RPMs of any fan fall below 1800 or if a fan has failed, an email is sent to the designated recipients. For more information on setting up email notification, see [“Setting Up Email Notifications” on page 34](#).

Viewing Temperature Status

To view temperature status, choose Monitoring and Notification > View Environmental Status > View Temperature Status from the navigation panel.

The View Temperature Status panel displays the temperature of the sensors in the NAS server. A green diamond in the Status column indicates that the unit is operating within the normal temperature range. A red diamond indicates that the temperature has exceeded the acceptable range. If the temperature rises above 55° Celsius (131° Fahrenheit), an email message is sent to the designated recipients. For more information on setting up email notification, see [“Setting Up Email Notifications” on page 34](#).

Note: You cannot change the temperature thresholds.

Viewing Power Supply Status

To display power supply status, choose Monitoring and Notification > View Environmental Status > View Power Supply Status from the navigation panel.

The View Power Supply Status panel has three columns showing power supply status. The Status column shows whether the power supply is functioning normally. The Voltage Warning and Temperature Warning columns show whether the voltage and temperature are at acceptable levels.

A green diamond in any of these columns indicates that the voltage or temperature levels are normal. A red diamond indicates that the voltage or temperature have exceeded the acceptable range. In this case, an email notification is sent to designated email notification recipients. For more information about email notification, see [“Setting Up Email Notifications” on page 34](#).

Viewing Voltage Status

To display the current voltage readings, choose Monitoring and Notification > View Environmental Status > View Voltage Regulator Status from the navigation panel.

[TABLE 10-3](#) lists 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
Baseboard 5VSB (Standby)	4.781V to 5.156V
Baseboard 12V	11.50V to 12.56V
Baseboard 12VRM	11.72V to 12.80V
Baseboard -12V	-12.62V to -10.97V
Baseboard VBAT	2.859V to 3.421V
SCSI A Term Pwr	4.455V to 5.01V
SCSI B Term Pwr	4.455V to 5.01V
Processor Vccp	1.116V to 1.884V

Viewing Usage Information

You can view usage information for file volumes, network activity, system activity, and network ports. The following sections are included:

- [“Viewing File Volume Usage” on page 165](#)
- [“Viewing Network Activity” on page 165](#)
- [“Viewing System Activity” on page 165](#)
- [“Viewing Network \(Port\) Statistics” on page 166](#)

Viewing File Volume Usage

To view the used and free space of file volumes in the system, choose Monitoring and Notification > View File Volume Usage from the navigation panel.

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

If a file volume is full (100 percent), you must remove checkpoints before you can delete files to free disk space. For more information, see [“Removing a Checkpoint” on page 181](#).

Viewing Network Activity

To display the number of I/O requests per second for all clients accessing the NAS appliance or gateway system, choose System Activity > View Networking Activity from the navigation panel.

Viewing System Activity

The NAS software monitors the activity and load of several devices throughout the storage system. The names and number of devices being monitored varies based on your hardware configuration.

To display the I/O requests for system devices, choose System Activity > View System Activity from the navigation panel.

The View System Activity panel lists activity for the system and network devices listed. For more information about the fields on this panel, see [“View System Activity Panel”](#) on page 416.

Viewing Network (Port) Statistics

To view network (port) statistics:

1. From the navigation panel, choose Network Configuration > Configure TCP/IP > Configure Network Adapters.

The Configure Network Adapters panel is displayed.

2. Select the port from the Adapter list.

The Interface and Statistics tabs display detailed statistics about the selected port. For more information, see [“Configure Network Adapters Panel”](#) on page 400.

Viewing Network Routes

Click a link below for information about network routes and how to view them:

- [“About Network Routes”](#) on page 166
- [“Displaying Routes”](#) on page 167

About Network Routes

There are two different kinds of routes: network routes and host routes. Network routes are used to send packets to any host on a particular network. Host routes are rarely used and are implemented to send packets to a host that is not attached to any known network, only to another host or gateway.

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

- u - route usable
- g - destination is a gateway
- h - host entry (net otherwise)
- r - host or net unreachable

- d – created dynamically (by redirect)
 - m – modified dynamically (by redirect)
 - D – message confirmed
 - M – subnet mask present
 - c – generate new routes on use
 - x – external daemon resolves name
 - l – generated by ARP or ESIS
 - S – manually added
 - 2 – protocol specific routing flag
 - 1 – protocol specific routing flag
-

Displaying Routes

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

The View the Routing Table Panel is displayed.

Monitoring System Status

You can monitor uninterruptible power supply (UPS), controller, and mirror status. For more information, see the following sections:

- [“About UPS Monitoring” on page 168](#)
- [“Enabling UPS Monitoring” on page 168](#)
- [“Viewing Controller Information” on page 169](#)
- [“Viewing the Mirror Status” on page 169](#)
- [“Viewing Mirroring Statistics” on page 169](#)

About UPS Monitoring

If you installed the unit with an uninterruptible power supply (UPS), you can monitor the UPS. UPS monitoring provides notification in the event of the following occurrences:

- **Power failure** – Indicates that a power failure occurred and the system is operating on battery power.
- **Power restoration** – Indicates that power was restored.
- **Low battery** – Indicates that the battery is low on power.
- **Recharged battery** – Indicates that the UPS has charged the battery to a normal level.
- **Battery replacement** – Indicates that the UPS has detected a battery defect such that replacement is necessary.
- **UPS alarms** – Indicates that the UPS has detected an ambient temperature or humidity outside of safe thresholds.
- **UPS failure** – Indicates that the system is unable to communicate with the UPS.

With UPS monitoring enabled, you will be notified of all errors through an error notification email, notification to the Simple Network Management Protocol (SNMP) server, display on the LCD panel, and display in the system log. The only exception to this is a recharged battery notification, which is sent through email, SNMP notification, and the system log display only. (There is no LCD panel notification.)

UPS monitoring can be enabled in a cluster configuration; however, only one NAS server can be connected to the UPS serial port. If that server goes down, no UPS monitoring will occur until the server is brought back up to a normal state, or the connection to the UPS serial port is physically moved to the surviving partner server. In addition, when both cluster servers are running in a normal state, the server that is not connected to the UPS serial port will repeatedly log a message telling you that UPS cannot open the COM port. You can ignore this message.

Enabling UPS Monitoring

To enable uninterruptible power supply (UPS) monitoring, first connect the UPS to the appliance or gateway system. If you do not connect the UPS before enabling monitoring, the monitoring system will notify you of a UPS failure:

1. From the navigation panel, choose Monitoring and Notification > Enable UPS Monitoring.

2. Select Enable UPS Monitoring.
3. Click Apply to save your change.

Viewing Controller Information

The read-only View Controller/Enclosure Information panel displays vendor, model, and firmware version information for each redundant array of independent disks (RAID) controller and expansion unit on the NAS device.

To view controller this display, choose RAID > View Controller/Enclosure Information from the navigation panel. Refer to [“View Controller/Enclosure Information Panel” on page 414](#) for detailed field descriptions.

Viewing the Mirror Status

To view the status of a mirror, choose File Replicator > Manage Mirrors from the navigation panel. The Sync State displays the current mirror status. For more information, see [“Manage Mirrors Panel” on page 355](#).

Viewing Mirroring Statistics

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

To view mirror statistics:

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

The system displays the status, incoming transactions, outgoing transactions, mirror buffer, and network statistics information for that mirrored file volume. For more information, see [“View Mirror Statistics Panel” on page 358](#).

System Maintenance

This chapter describes system maintenance functions. It includes the following sections:

- [“Setting Remote Access Options” on page 171](#)
- [“Configuring FTP Access” on page 172](#)
- [“Shutting Down the Server” on page 174](#)
- [“Locating a Drive or Controller/Expansion Unit” on page 174](#)
- [“Configuring the LAN Manager Compatibility Level” on page 175](#)
- [“Managing File-System Checkpoints” on page 176](#)
- [“Managing RAID Controllers” on page 184](#)
- [“Mounting File Systems” on page 186](#)
- [“Setting Up NDMP Backups” on page 186](#)
- [“Updating the Time Zone Database” on page 188](#)
- [“Enabling CATIA V4/V5 Character Translations” on page 189](#)
- [“Backing Up Configuration Information” on page 191](#)
- [“Upgrading NAS Software” on page 191](#)
- [“Configuring the Compliance Archiving Software” on page 194](#)
- [“Upgrading Array and Drive Firmware Revision Levels” on page 195](#)

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 Administrator, which uses the Secure Socket Layer (SSL) over Hyper Text Transfer Protocol (HTTP), and Secure Shell (ssh).

To set remote access security:

1. From the Web Administrator navigation panel, choose System Operations > Set Remote Access.
2. Check the Secure Mode checkbox for maximum security. In secure mode you can enable only Secure Web Administrator and Secure Shell by checking the associated checkbox.
3. If you are not using Secure Mode, select the checkbox for each service you want to enable:
 - Web Administrator
 - Telnet
 - Remote Login
 - Remote Shell
4. Click Apply.
5. If you have selected Secure Mode, restart the server for the settings to go into effect. For more information, see [“Shutting Down the Server” on page 174](#).

Configuring FTP Access

This section provides information about configuring File Transfer Protocol (FTP) access. The following subsections are included:

- [“About Configuring FTP Access” on page 172](#)
- [“Setting Up FTP Users” on page 173](#)

About Configuring FTP Access

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

You can set up three types of users:

- **Administrators**, who have the user name `admin` and use the same password used by graphical user interface (GUI) clients.

The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as the "/" symbol.

- **Users**, who have a user name and a password specified in the local password file or on a remote network information service (NIS), NIS+, or Lightweight Directory Access Protocol (LDAP) name server.

The user has access to all existing directories and files within the user's home directory. The home directory is defined as part of the user's account information and is retrieved by the name service.

- **Guests**, who log in with the user name `ftp` or its alias `anonymous`. The password for the `ftp` and `anonymous` user name is the email address of the guest user. All guest users have access to all directories and files within the home directory of the `ftp` user.

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

Setting Up FTP Users

To set up File Transfer Protocol (FTP) users:

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

Note: User names and passwords must be specified in the local password file or on a remote network information service (NIS), NIS+, or Lightweight Directory Access Protocol (LDAP) name server.
 - **Allow Admin Access** enables root access to those in possession of the administrative password (use with caution).

Note: A root user is a user with UID equal to 0 and the special Sun StorageTek user name, *admin*.
4. To enable logging, select the Enable Logging checkbox and specify the log file pathname.

The log file is saved to the exported volume you specify on the NAS server. For example, /vol1/ftplog will save the log file named ftplog to the directory /vol1.

5. Click Apply to save settings.

Shutting Down the Server

To shut down, halt, or reboot the server:

1. From the Web Administrator navigation panel, choose System Operations > Shut Down the Server.
2. Select the type of shutdown that you want to perform. For detailed information about the available shutdown options, see [“Shut Down the Server Panel” on page 430](#).





Caution: Check with Sun Services before selecting the Reboot Previous Version option.

3. Click Apply.

Locating a Drive or Controller/Expansion Unit

To locate a particular drive, controller unit, or expansion unit:

1. From the Web Administrator navigation panel, choose RAID > Manage RAID.
2. Click the Locate Drive or Locate Drive Tray button.
3. From the drive images shown, select (click on) the drive you want to locate, or any drive in the controller/expansion unit you want to locate.
4. Click the  button to cause the drive indicator lights to flash for the selected drive or controller/expansion unit.
5. After you physically locate the flashing drives, click the  button to stop the drive indicator lights from flashing.

Configuring the LAN Manager Compatibility Level

The NAS appliance or gateway system can be configured to run in either of two security modes under Windows: *Workgroup mode* or *NT domain mode*. The LAN Manager (LM) compatibility level controls the type of user authentication used in each mode, and is assigned as a numeric value in the range 1 through 5.

By default, the LM compatibility level is 3, which allows for authentication as follows:

- In Windows: Workgroup mode (also known as secure-share mode), the SMB server accepts LMv2/NTLMv2 responses, as well as LM/NTLM responses.
- In NT domain mode, the SMB Redirector running on the NAS device uses NTLMv2 authentication; that is, it sends both the LMv2 and NTLMv2 responses (respectively, as the case-insensitive and case-sensitive passwords) during SMB session setup.

For more information, go to the following web site and search for LM authentication and NTLM 2:

<http://support.microsoft.com>

You can change the LM compatibility level using the `lmcompatibility` subcommand of the `smbconfig` CLI command, as follows:

1. To view the current LM compatibility level, issue the `smbconfig lmcompatibility` command without any arguments:

```
smbconfig lmcompatibility
```

2. To set the LM compatibility level, use the `level` keyword, as shown below:

```
smbconfig lmcompatibility level=4
```

where 4 is the desired LM compatibility level, in the range 2 through 5, as detailed below:

Level	Sent by SMB Redirector (in NT Domain Mode)	Accepted by SMB Server (in Windows: Workgroup Mode)
2	NTLM	LM NTLM LMv2 NTLMv2
3	LMv2 NTLMv2	LLM NTLM LMv2 NTLMv2

Level	Sent by SMB Redirector (in NT Domain Mode)	Accepted by SMB Server (in Windows: Workgroup Mode)
4	LMv2 NTLMv2	NTLM LMv2 NTLMv2
5	LMv2 NTLMv2	LMv2 NTLMv2

Managing File-System Checkpoints

This section provides information about managing file-system checkpoints. The following subsections are included:

- [“About File-System Checkpoints” on page 176](#)
- [“Enabling File-System Checkpoints” on page 177](#)
- [“Scheduling File-System Checkpoints” on page 178](#)
- [“Creating a Manual Checkpoint” on page 180](#)
- [“Renaming a Checkpoint” on page 181](#)
- [“Removing a Checkpoint” on page 181](#)
- [“Sharing File-System Checkpoints” on page 182](#)
- [“Accessing Checkpoints” on page 183](#)

About File-System Checkpoints

A checkpoint is a virtual read-only copy of a file volume. A checkpoint is not an online backup. Checkpoints are used to:

- Retrieve data that is mistakenly modified or deleted. To do this, get access to the appropriate checkpoint, referring to [“Accessing Checkpoints” on page 183](#) for details.
- Stabilize backups. The NDMP backup software creates a special backup checkpoint from which it backs up the file volume, avoiding potential problems involved with backing up from the live file system.

Checkpoints are stored in the same physical location as the file volume, so if the file volume is lost, so are all its checkpoints.

Starting with NAS software version 4.20, you can store up to 256 checkpoints for each file volume. For file volumes that existed before upgrading to version 4.20, you are limited to 16 checkpoints unless you disable checkpoint processing (then enable it, as necessary). By disabling checkpoints, you initiate the conversion from 16-to-256 checkpoint support.

- If checkpoints were enabled for a specific file volume prior to upgrading to version 4.20, you can increase that limit to 256 by disabling checkpoints for the file volume, then enabling them again. You will lose all of the old checkpoints in this process.
- If checkpoints were disabled for a specific file volume prior to upgrading to version 4.20, you can increase the limit to 256 by first enabling checkpoints, then disabling them. This will remove any existing checkpoints. The 256 checkpoint limit will be available the next time checkpoints are enabled.

Checkpoints can be created manually, on a one-time basis, or they can be scheduled at regular intervals (for example, every evening at 11:00 p.m., or every Tuesday morning at midnight). File volumes remain operational during checkpoint processing.

A checkpoint is not created if the file volume is 90% full. If the file volume becomes 95%, checkpoints are deleted in expiration order until the volume is below 95% full or until there is only one checkpoint remaining.

At any time, you can view how many checkpoints are stored for a file volume and the total space used for checkpoints. Open File Volume Operations > Configure Checkpoints > Manage Checkpoints and look at the Status message at the top of the window to view this information.

Enabling File-System Checkpoints

Before you can create checkpoints for a file volume, you must enable checkpoint processing for that volume, as follows:

1. From the Web Administrator navigation panel, choose File Volume Operations > Edit Volume Properties.
2. From the Volumes list, select the volume for which you want to enable checkpoint processing
3. Select the Enable Checkpoints box.

4. If you plan to create NDMP backups for the file volume, select Use for Backups under Checkpoint Configuration. NDMP performs backups from a copy of the file volume, thereby avoiding potential problems involved with backing up from the live file system.
5. If you plan to create checkpoints for the file volume, select Automatic under Checkpoint Configuration. After selecting this box, the NAS software allows you to specify regularly scheduled checkpoints for that volume, as described under [“Scheduling File-System Checkpoints” on page 178](#).
6. Click Apply.

Scheduling File-System Checkpoints

This section provides information about scheduling file checkpoints. The following subsections are included:

- [“About Scheduling File-System Checkpoints” on page 178](#)
- [“Adding a Checkpoint to the Schedule” on page 179](#)
- [“Editing an Existing Checkpoint Schedule” on page 179](#)
- [“Removing a Schedule Line” on page 180](#)

About Scheduling File-System Checkpoints

The checkpoint schedule identifies days and times, weekly, when the NAS software creates a checkpoint. The schedule can contain up to five checkpoint requests for each file volume.

For each scheduled checkpoint, the schedule (available through File Volume Operations > Configure Checkpoints > Schedule Checkpoints) displays the name of the file volume, a description of the checkpoint, the scheduled times and days at which a checkpoint is taken, and the length of time for which the checkpoint is to be retained (days plus hours). The schedule looks like this, as displayed using Telnet for a single volume:

		Days		Hours AM	Hours PM	Keep	
Enabled	Description	SMTWTFS	M1234567890E	M1234567890E		Days	Hours
1.	Y	MTWTF5am5pm	-*****-	-----*-----	-----*-----	1	0
2.	Y	SunWed1pm	*--*---	-----	-*-----	0	12

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

Adding a Checkpoint to the Schedule

To add a checkpoint to the schedule, first enable checkpoints for the file volume, as described under [“Enabling File-System Checkpoints” on page 177](#). Then follow the steps below to add the new checkpoint:

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. Select the file volume to show the current schedule.
3. Click New to display the New Checkpoint Schedule window.
4. Click on the cell of the day/time grid to select that day and time. An unavailable cell indicates that an existing checkpoint is in effect for that time slot
5. Type a description for the checkpoint, such as “weekly” or “daily.”.This is a mandatory field.
6. Type the number of days and select the number of hours for which you want to retain the checkpoint.
7. Click Apply to save your changes.

Editing an Existing Checkpoint Schedule

To edit an existing checkpoint schedule:

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. Select the file volume to show the current schedule.
3. Click Edit to display the Edit Checkpoint Schedule window.
4. Click on the cell that identifies the checkpoint you want to change.
The Description and Keep fields display information for the current checkpoint.

5. Edit the checkpoint schedule, referring to [“Adding a Checkpoint to the Schedule” on page 179](#), as necessary.
6. Click Apply to save your changes.

Removing a Schedule Line

Follow these steps to remove a schedule line:

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Schedule Checkpoints.
2. Select the schedule entry that you want to remove and click Remove.

Note: Disabling checkpoints from the Edit Volume Properties panel has no effect on the schedule. If checkpoints are re-enabled, the schedule remains the same.

Creating a Manual Checkpoint

In addition to taking regularly scheduled checkpoints, you can request a manual (unscheduled) checkpoint at any time. To do this, first enable checkpoints for the file volume, as described under [“Enabling File-System Checkpoints” on page 177](#). Then use the Manage Checkpoints panel to create the manual checkpoint:

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Manage Checkpoints.
2. Click Create.
3. Use the drop-down menu to select the file volume you want.
4. Specify the checkpoint options. For detailed information about these options, see [“Create Checkpoint Window” on page 368](#).
5. Click Apply to create the checkpoint.

Renaming a Checkpoint

Follow these steps to rename a checkpoint:

Note: For automatic (scheduled) checkpoints, the NAS software depends on the system-assigned checkpoint name to identify the checkpoint, to retain it for the correct time period, and to delete it when it becomes stale. If you rename a scheduled checkpoint, it will be marked as a manual checkpoint, and it will not be deleted by the NAS software.

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Manage Checkpoints.
2. Select the checkpoint you want to rename.
3. Click Rename.
The Volume Name and Old Name fields are read-only.
4. Type the new name for the checkpoint.
5. Click Apply to save your changes.

Removing a Checkpoint

You can delete any checkpoint, regardless of whether it was created using the schedule, or manually.

Note: Backup checkpoints are only retained long enough to back up the file volume, and are deleted immediately thereafter by the backup software.

Note: If you disable checkpoint processing from the Edit Volume Properties panel, any checkpoints taken already will be deleted immediately, regardless of their defined retention.

To delete a checkpoint:

1. From the Web Administrator navigation panel, choose File Volume Operations > Configure Checkpoints > Manage Checkpoints.
2. Select the checkpoint you want to remove.
3. Click Remove.

Sharing File-System Checkpoints

Checkpoints can be shared, allowing network users to access the data that was current when the checkpoint was created. Follow these steps to share checkpoints:

1. From the Web Administrator navigation panel, choose Windows Configurations > Configure Shares.

Note: Alternatively, navigate to the checkpoint file volume under the System Manager, then right-click and choose the appropriate option from the pop-up menu (typically Sharing > New Share). Checkpoint volumes have a `.chkpnt` extension.

2. Click Add, then fill in the fields as described below.

For detailed information about these and other fields in this window, see [“New Share Window” on page 444](#).

3. Type the share name for the checkpoint in the Share Name box.

This is the name through which the checkpoint will be accessible from the network.

4. Click the Volume Name drop-down menu and select the checkpoint volume from the list. Checkpoint volumes have the `.chkpnt` extension.

5. Leave the Directory field blank.

6. If Active Directory Service (ADS) is enabled and configured, specify the Container field as the location in the ADS directory where the share will be published.

7. The following fields apply only if Windows Workgroup mode is enabled, as described under [“Configure Domains and Workgroups Panel” on page 452](#). If they are available, complete them as follows:

- User ID – Type 0.
- Group ID – Type 0.
- Umask – Type a three-digit value to specify the access permissions for the share, referring to [“About Share Access Permissions” on page 115](#) for field details.
- R/W Password and R/O Password – Leave blank (checkpoint volumes are read-only).

8. Click Apply.

The checkpoint share will be listed in the Configure Share panel.

Accessing Checkpoints

You can access file checkpoints as follows, to obtain the data that was current when the checkpoints were created.

1. Using a Windows network station, click Start -> Run.
2. Type the Internet Protocol (IP) address and checkpoint sharename for the NAS appliance or gateway-system server in the Run window. For example:

```
\\xxx.xxx.xxx.xxx\sharename.
```

3. Click OK.

Alternatively, you can access checkpoints through the “virtual” .chkpnt directory that exists for each directory in a file volume. This directory does not show up in directory listings, and can only be accessed if you specifically name it. To do this:

1. Export the directory to your local server, then navigate to the .chkpnt directory:

```
my-server# mount 192.168.75.55:V2 /mnt/v2
my-server# cd /mnt/v2
my-server# cd .chkpnt
```

2. List the checkpoint directories, where each directory is named after an individual checkpoint:

```
my-server# ls
checkpoint1 checkpoint2
```

3. Navigate to the checkpoint you want and list its contents. This represents the files as they existed when the checkpoint was taken:

```
my-server# cd checkpoint1
my-server# ls
test1.txt                xx2                        xxf
```

Managing RAID Controllers

This section provides information about using the `raidctl` command to manage redundant array of independent disks (RAID) controllers from the CLI. The command applies to Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems.

Controlling LEDs

Use the command described below to control redundant array of independent disks (RAID) controller LEDs for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems. Specify the variables as a particular *controller*, *tray*, or *slot* (also known as a column) number, respectively. Alternatively, specify 0..N to request all controllers, trays, or slots.

- To cause the LEDs in one or more trays to blink, enter:

```
raidctl locate type=lsi target=tray ctlr=controller tray=tray
```
- To cause the LEDs to blink in one or more drives, enter:

```
raidctl locate type=lsi target=drive ctlr=controller tray=tray slot=slot
```
- To stop blinking LEDs for one or more controllers, enter:

```
raidctl locate type=lsi action=stop ctlr=controller
```

To obtain Help on subcommands, enter **raidctl help** at the command line.

Getting Events and Configuration Information

Use the command described below to view redundant array of independent disks (RAID) controller events and configuration information for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems. Specify the *controller* variable as a particular controller number, or 0..N to request all controllers.

- To list the critical events for one or more controllers, enter:

```
raidctl get type=lsi target=events ctlr=controller etype=critical
```

The log of critical events is written to:

- For Sun StorageTek 5320 controller units, `/dvol/support/399x/ecri.txt`.

- For Sun StorageTek 5300 controller enclosures,
`/dvol/support/2882/ecri.txt`.

If the file already exists, you will be prompted to overwrite the file, specify a new file name, or cancel the operation.

- To display the configuration information on your terminal window, enter:

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

Alternatively, you can write the information to the file on your host (`profil.txt` in the example below):

```
rsh <server> raidctl get type=lsi target=profile  
ctlr=controller > profile.txt
```

- To list all events for one or more controllers (applicable only for NAS appliances; not for gateway systems), enter:

```
raidctl get type=lsi target=events ctlr=controller
```

The log of events is written to:

- For Sun StorageTek 5320 controller units, `/dvol/support/399x/eall.txt`.
- For Sun StorageTek 5300 controller enclosures,
`/dvol/support/2882/eall.txt`.

If the file already exists, you will be prompted to overwrite the file, specify a new file name, or cancel the operation.

To obtain Help on subcommands, enter **raidctl help** at the command line.

Setting the Controller Time and Battery Age

To set the redundant array of independent disks (RAID) controller time and battery age for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems. Specify the *controller* variable as a particular controller number, or 0..N to request all controllers.

- To reset the battery age for one or more controllers, enter:

```
raidctl set type=lsi target=battery-age ctlr=controller
```

- To synchronize the time with the server's time for one or more controllers, enter:

```
raidctl set type=lsi target=ctlr_time-age ctlr=controller
```

To obtain Help on subcommands, enter **raidctl help** at the command line.

Downloading RAID Array and Drive Firmware

To download redundant array of independent disks (RAID) array and drive firmware for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems, use the **raidctl download** command.

To obtain Help on subcommands, enter **raidctl help** at the command line.

Note: Refer to [“Upgrading Array and Drive Firmware Revision Levels” on page 195](#) for firmware upgrade procedures.

Mounting File Systems

After multiple continuous reboots, one or more file systems might become unmounted. To mount the file systems, issue the following CLI command:

```
mount -f volume-name
```

Do not mount or share the /cvol file system manually. Do not make modifications to /cvol using any method other than the Web Administrator or the console administration.

Note – Sun Services Engineers are authorized to perform a manual mount.

Setting Up NDMP Backups

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



Caution:In a cluster configuration, do not configure both heads to be in the same switch zone as the tape device. In the event of a head failover during a backup, data on the media is lost. Configure one of the heads to be in the same zone as the tape device.

By default, the current release uses V4 of NDMP, although V3 is supported and client systems can use V3. To verify the version, use the following command:

```
ndmp show version
```

To use V3, use the following command, but verify that no client systems use V4:

```
ndmp set version=3
```

To complete the configuration, you need to specify the complete paths to the devices. Use the following command to display the paths:

```
ndmp devices
```

To set up NDMP:

1. Configure the backup administration application to log in:
 - a. Enter the user name `admin`.
Note: In version 4.20, you specified the user name `administrator`.
 - b. Specify the same password used by the console administrator.
2. Configure the backup administration application to locate the devices on which the volumes reside. Specify the complete path to the device and the device's identifier, using the `ndmp devices` command.
Note: In version 4.20, you specified only the device's identifier.
3. For each file volume, verify that checkpoints are enabled and backup checkpoints are enabled. To view or set these settings, choose File Volume Operations > Edit Volume Properties
4. From the navigation panel, choose System Backup > Set Up NDMP.
5. Select the network interface card (NIC) port adapter or bond port used to transfer data to the backup tape drive (typically an interface configured with independent role).
6. Specify the full path, such as `/vol_ndmp`, for the directory used to store intermediate backup data and a permanent log of backup history. The directory must be independent from the volumes scheduled for backup, and at least 2 gigabytes in size.
7. Click Apply.

Updating the Time Zone Database

The NAS server supports the major world time zones and adjusts to local time. Different countries and regions set time in different ways. The NAS software uses the standard database format for the time zones.

Use the following procedure to update the time zone information:

1. From the `ftp://elsie.nci.nih.gov/pub/` site, download the latest file, for example, `tzdata2007c.tar.gz`.
2. Use `gunzip` and `tar` to extract the database files. The extracted files refer to the various regions as shown in [TABLE 11-1](#). If a file name has more than eight characters, it must be renamed to meet the eight-character limit of the `/cvol` directory.

TABLE 11-1 Time Zone Database Files

Continent/Region	File Name	
Africa	africa	africa
Antarctica	antarctica	antarcti
Asia and Australia	australasia	australa
Pacific Islands	pacificnew	pacificn
Greenwich Mean Time (GMT) offset only (no Daylight Savings).	etcetera	etcetera
European countries	europe	europe
North America	northamerica	northame
Special time corrections made in 1987 for Saudi Arabia	solar87	solar87
South America	southamerica	southame

3. Determine the current boot directory. Check the `/cvol/defstart` file; a value of 1 indicates `nf1` and a value of 2 indicates `nf2` as the boot directory.
4. Create the `tz` directory in the current boot directory.
5. Copy the files to `cvol/nf1/tz` or `cvol/nf2/tz`, as appropriate.

6. Use the `zic` command to install the timezone database file for your region. For example, the following command installs the northamerica timezones in the `nf2` boot directory:

```
zic /cvol/nf2/tz/northame
```

A reboot is not required for the new time zones to take effect.

Enabling CATIA V4/V5 Character Translations

NAS appliances and gateway systems inter-operate with CATIA V4/V5 products (developed by Dessault Systèmes). The following sections provide information about the CATIA software:

- [“About CATIA V4/V5 Character Translations” on page 189](#)
- [“Enabling CATIA Manually” on page 190](#)
- [“Enabling CATIA Automatically” on page 190](#)

About CATIA V4/V5 Character Translations

NAS appliances and gateway systems inter-operate with CATIA V4/V5 products (developed by Dessault Systèmes).

CATIA V4 is a Unix-only product, whereas CATIA V5 is available on both Unix and Windows platforms. CATIA V4 might 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 inter-operability.

The translation table is shown in [TABLE 11-2](#).

TABLE 11-2 CATIA Character Translation Table

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

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

Enabling CATIA Manually

You must re-enable CATIA support after each system reboot.

To enable CATI, issue the command:

```
load catia.
```

Enabling CATIA Automatically

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
```

Backing Up Configuration Information

After you configure the NAS OS or modify the NAS OS configuration, follow the steps below to back up the configuration settings. In a cluster configuration, it is only necessary to perform these steps on one server, because the configuration is synchronized between servers.

1. At the CLI command line, enter `load unixtools`.
2. Type `cp -r v /dvol/etc backup-path`, where *backup-path* is the full path, including the volume name, of the desired directory location of the configuration file backup. The directory must already exist and be empty.

This copies all of the configuration information stored in the `/dvol/etc` directory to the designated location.

Upgrading NAS Software

The discussion describes how to upgrade the NAS software, as follows.

- [“Upgrading Software With a Reboot” on page 192](#) tells how to upgrade NAS appliance or gateway system software, then reboot the server for the changes to take effect.
- [“Upgrading Cluster Software Without Interrupting Service” on page 192](#) tells how to upgrade NAS software in a cluster configuration, such that the service is never brought down.



Caution: Never update system software when the RAID subsystem is in a critical state (such as after a drive fails), creating a new volume, or rebuilding an existing volume. You can see this information in the system log, or from the Web Administrator RAID display.

Upgrading Software With a Reboot

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

Note: In a cluster configuration, perform this procedure on both servers in the cluster before you reboot the server. The cluster must be in optimal mode prior to the update.

Follow these steps to update the Sun StorageTek NAS software on your appliance or gateway system:

1. Download the latest version of the NAS software, available at www.sunsolve.sun.com. If you are unsure of which version to download, contact Sun Services to get the appropriate files for your system configuration.
2. From the Web Administrator navigation panel, choose System Operations > Update Software.
3. In the Update Software panel, type the path where the update files are located. If you need to look for the path, click Browse.
4. Click Update to start the process.
5. 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.

When upgrading to a release that is 4.10 or higher, from a release earlier than 4.10, you will be asked to re-enter time zone information, even though it was previously entered. This is due to a changed implementation that offers additional time zone locations.

Upgrading Cluster Software Without Interrupting Service

Follow these steps to upgrade the Sun StorageTek NAS software on in a cluster configuration, such that the service is never brought down. This is known as a *rolling upgrade*.

This procedure supports a single NAS OS software revision upgrade, for example 4.12 to 4.21. Perform upgrades that span more than one release incrementally, checking the OS release notes for each release to determine any issues or potential downtime.

1. From a remote web browser window, log in to the Web Administrator GUI on the first server in the cluster (in this example, Server 1). As necessary, refer to [“Logging In” on page 2](#) for instructions.
2. From the Web Administrator navigation panel, choose System Operations > Update Software.
3. Browse to select a valid OS image file, then click Update. This copies the image file to Server 1 and upgrades the NAS OS software.
4. When the upgrade is finished, a pop-up dialog prompts you to reboot the server manually. Click OK to close this dialog.
5. From the Web Administrator navigation panel, select System Operations > Shut Down the Server.
6. Select Reboot This Head and click Apply.
7. Close the web browser window.
8. Looking at the LCD panel, verify that Server 1 (Head 1) has restarted and is in the QUIET state.
9. From a remote web browser window, log in to the Web GUI on the second server in the cluster (Server 2).
10. Looking at the LCD panel, verify that Server 2 (Head 2) is in the ALONE state. You can also verify this using Web Administrator.
11. From the Web Administrator navigation panel, choose High Availability > Recover, then click the Recover button. Wait for the recovery to complete.
Under a heavy processing load, some LUNs might not be fully restored. Repeat this step if any LUN remains in the failover state.
12. Verify that both servers are in the NORMAL state (using the LCD panel or Web Administrator).
13. From the Web Administrator navigation panel, choose System Operations > Update Software.
14. Browse to select the same OS image file used in [Step 3](#), then click Update. This copies the image file to Server 2 and upgrades the NAS OS software.
15. When the upgrade is finished, a pop-up dialog prompts you to reboot the server manually. Select No.

16. From the Web Administrator navigation panel, choose System Operations > Shut Down the Server.
17. Select Reboot This Head and click Apply.
18. Close the web browser window.
19. Looking at the LCD panel, verify that Server 2 (Head 2) has restarted and is in the QUIET state.
20. From a remote web browser window, log in to the Web GUI on Server 1.
21. Verify that Server 1 (Head 1) is in the ALONE state.
22. From the Web Administrator navigation panel, choose High Availability > Recover, then click the Recover button. Wait for the recovery to complete.
23. Verify that both servers are in the NORMAL state, and running the new OS version. You can check the OS version on the Web Administrator startup System Status panel.

When upgrading to a release that is 4.10 or higher, from a release earlier than 4.10, you will be asked to re-enter time zone information, even though it was previously entered. This is due to a changed implementation that offers additional time zone locations.

Configuring the Compliance Archiving Software

If you have purchased, activated, and enabled the Compliance Archiving Software option (see [“Activating System Options” on page 131](#)), there are additional settings you can establish using the command-line interface.

Note: Gateway-system configurations support advisory compliance but not mandatory compliance.

Changing the Default Retention Period

Enter this CLI command to change the default retention period:

```
fsctl compliance volume drt time
```

where *volume* is the name of the volume for which you want to set the default retention time, and *time* is the duration of the default retention time in seconds.

To set the default retention to "permanent," use the maximum allowable value, 2147483647.

Enabling CIFS Compliance

In its initial configuration, the Compliance Archiving Software supports data retention requests only from NFS clients. Enter this CLI command to enable Windows Common Internet File System (CIFS) clients to access to this functionality:

```
fsctl compliance wte on
```

Upgrading Array and Drive Firmware Revision Levels

This section explains how to determine current array and drive firmware revision levels for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems, and how to upgrade your firmware. For purposes of this discussion, the term "array and drive firmware" refers to the firmware loaded on the redundant array of independent disks (RAID) controller, controller NVSRAM, expansion unit, and drive for a storage array – as appropriate to your installation.

This section contains the following topics:

- ["Determining If You Need to Upgrade the Firmware" on page 196](#)
- ["Upgrading Array and Drive Firmware \(Reboot Required\)" on page 196](#)
- ["Upgrading Array Firmware \(No Reboot Required\)" on page 199](#)
- ["Upgrading Drive Firmware \(Reboot Required\)" on page 204](#)
- ["Capturing raidctl Command Output" on page 205](#)

Determining If You Need to Upgrade the Firmware

Before you begin a firmware upgrade, decide if an upgrade is required by determining the current firmware revision level for each array component.

You can use the `raidctl profile` command to capture and record the current firmware revision level of each redundant array of independent disks (RAID) controller, controller NVSRAM, expansion unit, and drive. See [“Capturing `raidctl` Command Output” on page 205](#) for more information.

Upgrading Array and Drive Firmware (Reboot Required)

Use this procedure to upgrade redundant array of independent disks (RAID) array and drive firmware. This procedure requires you to reboot the NAS server.

If you cannot reboot the NAS server and need to upgrade only array firmware, refer to [“Upgrading Array Firmware \(No Reboot Required\)” on page 199](#).

The amount of time required to complete a firmware upgrade will vary, depending on your configuration. For example, it takes approximately 50 minutes to upgrade and reboot a single NAS server with one controller unit, one Fibre Channel (FC) expansion unit, and one Serial Advanced Technology Attachment (SATA) expansion unit. See [Step 13 on page 201](#) to determine how much time to allow for your configuration.

Note: Upgrading drive firmware always requires a reboot of the NAS server.

Note: All drives of each drive type will be upgraded, including those that are already at the firmware level of the current firmware file.



Caution: Do not update drive firmware when the RAID subsystem is in critical state (such as after a drive fails), creating a new volume, or rebuilding an existing volume. You can see this information in the system log, or from the Web Administrator RAID display.

Before you begin this procedure, make sure that the NAS server software version 4.10 Build 18 (minimum) is installed. Do not attempt to upgrade array and drive firmware for a NAS server that has a previous software version. If the NAS server software is at an earlier version, go to www.sunsolve.sun.com to obtain the latest software version.

To upgrade array and drive firmware:

1. Download the latest patch from www.sunsolve.sun.com and unzip the file.
2. Review the patch `readme` file to determine which firmware revision levels are associated with the patch.
3. From a NAS client, enable FTP.

For information about how to enable FTP using the GUI, see “[About Configuring FTP Access](#)” on page 172. Refer to [See “Configuring File Transfer Protocol \(FTP\) Access”](#) on page 292. if you are using the CLI.

4. Change to the directory to which you downloaded the patch.
5. Use FTP to connect to the NAS server, and log in as the admin user.
6. Enter `bin` for binary mode.
7. At the `ftp` prompt, create the following directories on `/cvol` by issuing these commands:

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

8. Change to the directory you created for the firmware and copy the firmware file (see [TABLE 11-3](#)) using the `put` command.

For example, to load firmware for the RAID controller, issue the following commands:

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

Note: The firmware file names are truncated after they are copied to their associated directories.

9. Continue to load each firmware file to the appropriate directory.

TABLE 11-3 lists the directory and example firmware file for each component.

TABLE 11-3 Component Firmware Directories and Files

Component	Directory	Example File Name
RAID controller	/cvol/firmware/2882/ctrlr	SNAP_288X_06120910.dlp
RAID controller NVSRAM	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
FC expansion unit	/cvol/firmware/2882/jbod	esm9631.s3r
SATA expansion unit	/cvol/firmware/2882/jbod	esm9722.dl
Drive types:		
Seagate ST314680	/cvol/firmware/2882/drive	D_ST314680FSUN146G_0407.dlp
Seagate 10K	/cvol/firmware/2882/drive	D_ST314670FSUN146G_055A.dlp
Hitachi 400GB HDS724040KLSA80	/cvol/firmware/2882/drive	D_HDS7240SBSUN400G_AC7A.dlp
Fujitsu MAT3300F 300GB	/cvol/firmware/2882/drive	D_MAT3300FSUN300G_1203.dlp
Seagate 10K 300GB	/cvol/firmware/2882/drive	D_ST330000FSUN300G_055A.dlp

10. Log out of the FTP session.

11. Use Telnet to connect to the NAS server, and log in to a user account with admin privileges.

12. Reboot the system. For a cluster configuration, reboot both servers.

The following table provides the approximate time needed to upgrade the firmware for each component.

Component	Time to Complete Upgrade
RAID controller	Reboot plus 15 minutes
RAID controller NVSRAM	Reboot plus 5 minutes
FC or SATA expansion unit	Reboot plus 5 minutes
Drives	Reboot plus 1.5 minutes per drive

13. Verify that the new firmware has been loaded by issuing this command:

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

You can also check the system log for failures.

Upgrading Array Firmware (No Reboot Required)

This procedure upgrades redundant array of independent disks (RAID) array firmware without requiring a reboot of the NAS server.

Before you begin this procedure, keep the following in mind:

- NAS server software version 4.10 Build 18 (minimum) must be installed. Do not attempt to upgrade firmware to a NAS server that has a previous software version.
- This procedure is best performed with limited I/O activity. The controller unit will quiesce I/O during this procedure.



Caution: Do not update drive firmware when the RAID subsystem is in critical state (such as after a drive fails), creating a new volume, or rebuilding an existing volume. You can see this information in the system log, or from the Web Administrator RAID display.

To upgrade array firmware, with no reboot required:

1. Download the latest patch from www.sunsolve.sun.com and unzip the file.
2. Review the patch `readme` file to determine which firmware revision levels are associated with the patch.
3. Gather the tray ID for each expansion unit that requires a firmware upgrade.
 - a. From the Web Administrator, go to RAID > View Controller/Enclosure Information.
 - b. Select the appropriate RAID controller from the Controller Information box.
 - c. The Enclosures Information area displays the tray ID for each controller unit and expansion unit that is managed by the selected controller. Tray IDs are relative to, and unique within, the array managed by the controller unit that houses the selected controller.

For expansion units, the Firmware Release field the revision level. This is the tray ID you will need to upgrade the firmware.

Note: For controller units, the Firmware Release field displays <N/A>.

4. Change to the directory to which you downloaded the patch.
5. From a NAS client, enable FTP.

For information about how to enable FTP using the GUI, see [“About Configuring FTP Access” on page 172](#). Refer to [“Configuring File Transfer Protocol \(FTP\) Access” on page 292](#) if you are using the CLI.

6. Use FTP to connect to the NAS server, and log in to a user account with admin privileges.
7. Enter `bin` for binary mode.
8. At the `ftp` prompt, create the following directories on `/cvol` by issuing these commands:

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

9. Load each firmware file to the appropriate directory. The following table lists the directory and example firmware file for each component.

Component	Directory	Example File Name
RAID controller	<code>/cvol/firmware/2882/ctlr</code>	<code>SNAP_288X_06120910.dlp</code>
RAID controller NVS RAM	<code>/cvol/firmware/2882/nvsram</code>	<code>N2882-612843-503.dlp</code>
FC expansion unit	<code>/cvol/firmware/2882/jbod</code>	<code>esm9631.s3r</code>
SATA expansion unit	<code>/cvol/firmware/2882/jbod</code>	<code>esm9722.dl</code>

For each file, change to the directory you created for the firmware, then copy the firmware file using the `put` command. For example, to load firmware for the RAID controller, issue the following commands:

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

10. Log out of the FTP session.
11. Use Telnet to connect to the NAS server, and log in to a user account with admin privileges.
12. Use the `raidctl download` command to load each file to the target directory.
Note: For `raidctl` command usage, enter `raidctl` with no arguments at the command line.

To load the RAID controller firmware from the `ctlr` directory to controller 0 and 1, issue the following command:


```
raidctl download type=lsi target=ctlr ctlr=0,1
```

This command downloads the firmware file to both RAID controllers and removes the file from the directory.

Note: The `raidctl download` command deletes the component-specific firmware file from `/cvol/firmware/2882` after each successful invocation of the command. For example, the `/cvol/firmware/2882/ctlr` file is deleted after each successful invocation of the `raidctl download type=lsi target=ctlr ctlr=0` command. Therefore, you must re-copy the firmware file after upgrading each component (controller unit, controller NVSRAM, expansion unit, and drives) if you have multiple controller units or expansion units. With two controller units, the second unit is specified as `ctlr=2` in the command `raidctl download type=lsi target=ctlr ctlr=2`.

To download NVSRAM, issue this command:

```
raidctl download type=lsi target=nvsram ctlr=0
```

To download the firmware located in the `jbod` directory to expansion unit 0 in tray 1, issue this command:

```
raidctl download type=lsi target=jbod ctlr=0 tray=1
```

13. Monitor the progress of each download from the Telnet session.

The approximate time needed to complete each upgrade is as follows:

Component	Minutes per Component
RAID controller	15 minutes
RAID controller NVSRAM	5 minutes
FC or SATA expansion unit	5 minutes

Note: After the upgrades are complete, the Telnet cursor can take up to 5 minutes to return. Wait during this time until the cursor is displayed.

14. Before continuing to the next component, verify in the system log that the download is complete.

The following example shows output from the system log:

```
Ctrl-  
  
Firmware Download 90% complete  
Firmware Download 95% complete  
Firmware Download 100% complete  
Waiting for controllers to become ACTIVE  
Controller 0 - now ACTIVE  
Controller 1 - now ACTIVE  
Controllers are now active  
nvram-
```

```

raidctl download type=lsi target=nvsram ctr=0
Flashing C0 NVSRAM: /cvol/nf2/./firmware/2882/nvsram/n2882-61.dlp
(48068)
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
ESM-
>> raidctl download type=lsi target=jbod ctr=0 tray=1

Flashing C0 JBOD 1 with /cvol/nf1/./firmware/2882/jbod/esm9631.s3r
(663604)
Firmware Download 20% complete
Firmware Download 30% complete
Firmware Download 50% complete
Firmware Download 60% complete
Firmware Download 90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download 20% complete
10/26/05 10:57:46 I Firmware Download 30% complete
10/26/05 10:57:50 I Firmware Download 40% complete
10/26/05 10:57:54 I Firmware Download 50% complete
10/26/05 10:57:58 I Firmware Download 60% complete
10/26/05 10:58:03 I Firmware Download 70% complete
10/26/05 10:58:08 I Firmware Download 80% complete
10/26/05 10:58:13 I Firmware Download 90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives

```

Upgrading Drive Firmware (Reboot Required)

Use this procedure to upgrade only drive firmware. This procedure requires you to reboot the NAS server.

Note: Upgrading drive firmware always requires a reboot of the NAS server.

Note: All drives of each drive type will be upgraded, including those that are already at the firmware level of the current firmware file.

The amount of time required to complete a firmware upgrade will vary, depending on the number of drives that are installed plus the time it takes to reboot the NAS server. See [Step 13](#) on [page 201](#) to determine how much time to allow for your configuration.



Caution: Do not update drive firmware when the RAID subsystem is in critical state (such as after a drive fails), creating a new volume, or rebuilding an existing volume. You can see this information in the system log, or from the Web Administrator RAID display.

Before you begin a drive firmware upgrade, make sure that the NAS server software 4.10 Build 18 (minimum) is installed. Do not attempt to upgrade firmware to a NAS server that has a previous software version.

To upgrade drive firmware, with a reboot required:

1. Download the latest patch from www.sunsolve.sun.com and unzip the file.
2. Review the patch readme file to determine which firmware revision levels are associated with the patch.
3. Change to the directory to which you downloaded the patch.

4. From a NAS client, enable FTP.

For information about how to enable FTP, see [“About Configuring FTP Access” on page 172](#) or [“Configuring File Transfer Protocol \(FTP\) Access” on page 292](#).

5. Use FTP to connect to the NAS server and log in as the admin user.
6. Enter bin for binary mode.
7. At the ftp prompt, create the following directory on /cvol by issuing this command:

```
mkdir /cvol/firmware/2882/drive
```

8. Change to the directory you created for the drive firmware and copy the drive firmware files (see [TABLE 11-3](#)) using the `put` command.
For example, to load firmware for the Seagate ST314680 drive issue the following commands:

```
cd /cvol/firmware/2882/drive
put D_ST314680FSUN146G_0407.dlp
```
9. Log out of the FTP session.
10. Use Telnet to connect to the NAS server and log in as the `admin` user.
11. Reboot the system. For a cluster configuration, reboot both servers.
The approximate time to complete the upgrade is reboot time plus 1.5 minutes for each drive.
12. Verify that the new firmware has been loaded by issuing this command:

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

You can also check the system log for failures.

Capturing `raidctl` Command Output

You can use the `raidctl profile` command to determine the current firmware revision level of each controller unit, controller NVSRAM, expansion unit, and drive. This section provides instructions in the following procedures:

- [“Capturing `raidctl` Command Output From a Solaris Client” on page 205](#)
- [“Capturing `raidctl` Output From a Windows Client” on page 216](#)

Capturing `raidctl` Command Output From a Solaris Client

To capture `raidctl` command and output from a Solaris client:

1. From a Solaris client, type the `script` command and a file name. For example:

```
> script raidctl
```
2. Use Telnet to connect to the NAS server.
3. Type the following `raidctl` command to collect the output:

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

With two controller units, the second unit is specified as `ctrl=2`, as shown in the following example:

```
raidctl get type=lsi target=profile ctrl=2
```

4. Type `exit` to close the Telnet session.
5. Type `exit` again to close the file named `raidctl`.

The following example shows command output, with the command and resulting firmware levels in bold:

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *****
5310 > raidctl get type=lsi target=profile ctrl=0

SUMMARY-----
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
    Number of standard volumes: 4
    Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
    Standby: 2
    In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
    Firmware version: PkgInfo 06.12.09.10
    NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS -----
Number of controllers: 2

Controller in Tray 0, Slot B
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
  Board ID: 2882
  Product ID: CSM100_R_FC
  Product revision: 0612
  Serial number: 1T44155753
  Date of manufacture: Sat Oct 16 00:00:00 2004
  Cache/processor size (MB): 896/128
  Date/Time: Thu Nov 2 19:15:49 2006
  Associated Volumes (* = Perferred Owner):
    lun4* (LUN 3)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C7.A7
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.106
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
```

```
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
```



```
Board ID: 2882
Product ID: CSM100_R_FC
Product revision: 0612
Serial number: 1T44155741
Date of manufacture: Sun Oct 10 00:00:00 2004
Cache/processor size (MB): 896/128
Date/Time: Thu Nov  2 19:15:45 2006
Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C6.F9
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.105
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 1
  Current ID: 255/0x0
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
```

```
Link status: Down
  Topology: Unknown
  World-wide port name: 20:06:00:A0:B8:16:C6:FA
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 1
  Current ID: 255/0x0
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
World-wide node name: 20:06:00:A0:B8:16:C6:F9
Part type: HPFC-5400      revision 6
```

VOLUME GROUPS-----

```
Number of volume groups: 4
Volume group 1 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun1 (681 GB)
  Associated drives (in piece order):
    Drive at Tray 0, Slot 7
    Drive at Tray 0, Slot 6
    Drive at Tray 0, Slot 5
    Drive at Tray 0, Slot 4
    Drive at Tray 0, Slot 3
    Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun2 (681 GB)
  Associated drives (in piece order):
    Drive at Tray 0, Slot 14
    Drive at Tray 0, Slot 13
    Drive at Tray 0, Slot 12
    Drive at Tray 0, Slot 11
    Drive at Tray 0, Slot 10
    Drive at Tray 0, Slot 9
```

Volume group 3 (RAID 5)
 Status: Online
 Tray loss protection: No
 Associated volumes and free capacities:
 lun3 (817 GB)
 Associated drives (in piece order):
 Drive at Tray 11, Slot 5
 Drive at Tray 11, Slot 4
 Drive at Tray 11, Slot 3
 Drive at Tray 11, Slot 2
 Drive at Tray 11, Slot 1
 Drive at Tray 11, Slot 7
 Drive at Tray 11, Slot 6

Volume group 4 (RAID 5)
 Status: Online
 Tray loss protection: No
 Associated volumes and free capacities:
 lun4 (817 GB)
 Associated drives (in piece order):
 Drive at Tray 11, Slot 13
 Drive at Tray 11, Slot 12
 Drive at Tray 11, Slot 11
 Drive at Tray 11, Slot 10
 Drive at Tray 11, Slot 9
 Drive at Tray 11, Slot 8
 Drive at Tray 11, Slot 14

STANDARD VOLUMES-----

SUMMARY

Number of standard volumes: 4

NAME	STATUS	CAPACITY	RAID	LEVEL	VOLUME GROUP
lun1	Optimal	681	GB	5	1
lun2	Optimal	681	GB	5	2
lun3	Optimal	817	GB	5	3
lun4	Optimal	817	GB	5	4

DETAILS

Volume name: lun1

Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A

Subsystem ID (SSID): 0

Status: Optimal

Action: 1

Tray loss protection: No

Preferred owner: Controller in slot A

Current owner: Controller in slot B

Capacity: 681 GB

RAID level: 5

Segment size: 64 KB

Associated volume group: 1

Read cache: Enabled

Write cache: Enabled

Flush write cache after (in seconds): 8

Cache read ahead multiplier: 1

Enable background media scan: Enabled

Media scan with redundancy check: Disabled

DRIVES-----

SUMMARY

Number of drives: 28

Supported drive types: Fiber (28)

BASIC:

CURRENT	PRODUCT	FIRMWARE			
TRAY, SLOT	STATUS	CAPACITY	DATA RATE	ID	REV
0,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307

11,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307

HOT SPARE COVERAGE:

The following volume groups are not protected:

Total hot spare drives: 2
 Standby: 2
 In use: 0

DETAILS:

Drive at Tray 0, Slot 1 (HotSpare)
 Available: 0
 Drive path redundancy: OK
 Status: Optimal
 Raw capacity: 136 GB
 Usable capacity: 136 GB
 Product ID: ST314680FSUN146G
 Firmware version: 0307
 Serial number: 3HY90HWJ00007510RKKV

Vendor: SEAGATE

Date of manufacture: Sat Sep 18 00:00:00 2004
 World-wide name: 20:00:00:11:C6:0D:BA:3E
 Drive type: Fiber
 Speed: 10033 RPM
 Associated volume group: None
 Available: No

Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:CA:12
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive at Tray 11, Slot 1

Drive path redundancy: OK
Status: Optimal
Raw capacity: 136 GB
Usable capacity: 136 GB
Product ID: ST314680FSUN146G
Firmware version: 0307
Serial number: 3HY90JEW00007511BDPL
Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:C8:8B
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive Tray 1 Overall Component Information

Tray technology: Fibre Channel
Minihub datarate mismatch: 0
Part number: PN 54062390150
Serial number: SN 0447AWF011
Vendor: VN SUN
Date of manufacture: Mon Nov 1 00:00:00 2004
Tray path redundancy: OK
Tray ID: 11

Tray ID Conflict: 0

Tray ID Mismatch: 0
Tray ESM Version Mismatch: 0
Fan canister: Optimal
Fan canister: Optimal
Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A6847502330F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A6847502330F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A68475023N0F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Temperature: Optimal

Temperature: Optimal

Esm card

Status: Optimal
Firmware version: 9631
Maximum data rate: 2 Gbps
Current data rate: 2 Gbps
Location: A (left canister)
Working channel: -1
Product ID: CSM100_E_FC_S
Part number: PN 37532180150
Serial number: SN 1T44462572
Vendor: SUN
FRU type: FT SBOD_CEM
Date of manufacture: Fri Oct 1 00:00:00 2004

Esm card

Status: Optimal
Firmware version: 9631
Maximum data rate: 2 Gbps
Current data rate: 2 Gbps
Location: B (right canister)
Working channel: -1

Capturing `raidctl` Output From a Windows Client

To capture `raidctl` output from a Windows client:

1. Click Start > Run and type `cmd`. Click OK.
2. Right-click at the top of the window and choose Properties.
The Properties window is displayed.
3. Change the Screen Buffer size (height) to 3000.
4. Click the Options tab and deselect Insert Mode.
5. Use Telnet to connect to the NAS server, and type the following `raidctl` command to collect the output:
`raidctl get type=lsi target=profile ctrl=0`
6. Copy the text to a file using any text editor. For example:
 - a. Select the output text and Press Ctrl-C to copy the data.
 - b. Open WordPad by clicking Start > Programs > Accessories > WordPad.
 - c. Click in the window and press Ctrl-V to paste the text.
 - d. Save the file.
7. Open the file and search for the current firmware version for each component.

Replacing Components

This chapter provides replacement procedures for customer-replaceable units (CRUs). It includes the following sections:

- [“Tools and Supplies Needed” on page 217](#)
- [“Powering Off” on page 218](#)
- [“Removing the Covers” on page 220](#)
- [“Locations of Customer-Replaceable Units” on page 224](#)
- [“Replacing Components” on page 224](#)

Tools and Supplies Needed

The NAS server can be serviced with the following items:

- No. 2 Phillips screwdriver
- Antistatic wrist strap
- Ballpoint pen or other stylus (to press the recessed Power button)
- 8-mm nut-driver (for motherboard replacement)

Powering Off

1. **Choose a method for shutting down the appliance from main power mode to standby power mode.**
 - **Local shutdown** -- Use the LCD display, as shown in [FIGURE 12-1](#) to perform a graceful shutdown of the appliance under operating system control. Press any LCD button to change the display to the following menu:
 - A. Network Config
 - B. Shutdown ServerSelect Shutdown Server and then select Power Off.
 - **Remote shutdown** -- From the Web Administrator interface, select System Operations > Shut Down to perform a graceful shutdown.



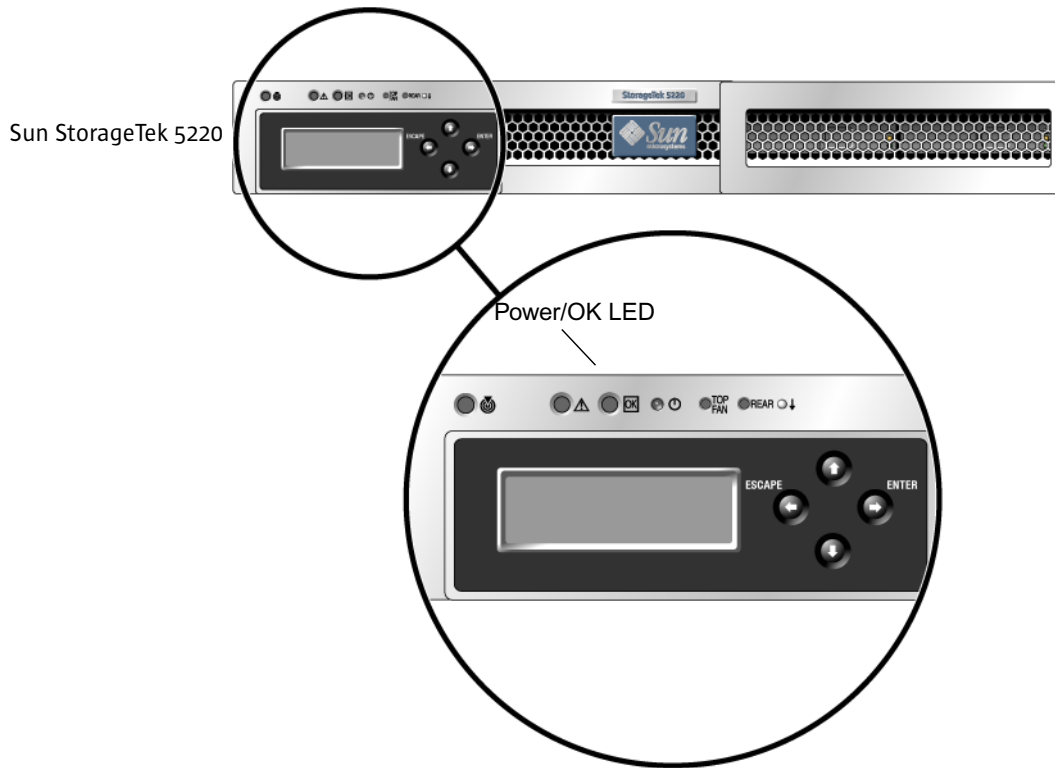
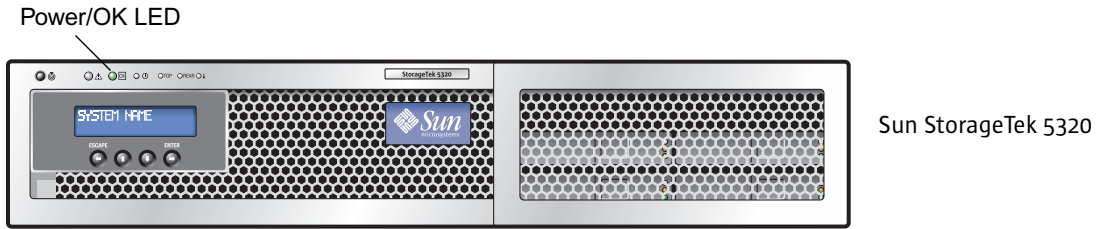
Caution – Do not use the power button to shut down the system. Always use the LCD display or remote shutdown procedure. Improper shutdown can result in a loss of data.

2. **When main power is off, the Power/OK LED on the front panel flashes, indicating that the appliance is in standby power mode.**



Caution – When you use the LCD display to enter standby power mode, power is still directed to the service processor and power supply fans. To completely power off, you must disconnect the AC power cords from the back panel.

FIGURE 12-1 Location of Power/OK LED



3. Unplug both power cords from the appliance's power supplies.
4. Turn off all peripheral devices connected to the system.
5. Label any peripheral cables and/or telecommunication lines that you must disconnect in order to remove and replace a specific component.

Removing the Covers



Caution: Before handling components, attach an electrostatic discharge (ESD) wrist strap to the grounding post that is built into the back of the chassis. The system's printed circuit boards and hard disk drives contain components that are extremely sensitive to static electricity.

Removing the Main Cover

1. Press down on the cover release and, using the indent for leverage, slide the main cover toward the back of the chassis, approximately 0.5 inch (12 mm). See [FIGURE 12-2](#).
2. Grasp the cover by its back edge and lift it straight up from the chassis.

Note: When you remove any cover, the intrusion switch that is on the front I/O board automatically powers down the system to standby mode.

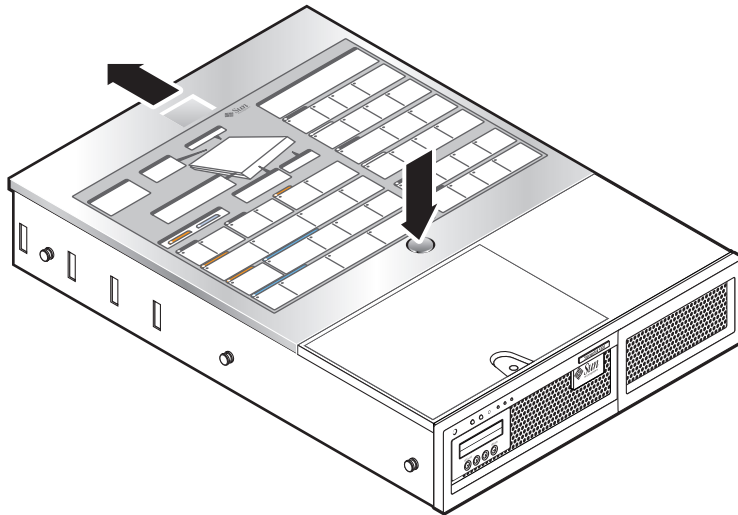


FIGURE 12-2 Removing the Main Cover

Removing the Front Bezel

[FIGURE 12-3](#) shows the procedure for a Sun StorageTek 5320 appliance. The Sun StorageTek 5220 Appliance has the same fan bay door and captive screw.

Remove the bezel from the front of the chassis by following these steps.

1. Open the fan bay door and use a No. 2 Phillips screwdriver to unfasten the captive screw that locks the bezel in place. See [FIGURE 12-3](#).
2. Grasp the outer edges of the bezel and gradually ease the bezel away 1 inch (2.4 cm) from the chassis.



Caution: A 3-inch USB cable is attached to the LCD on the back side of the bezel. Be careful not to force the bezel from the chassis.

3. Disconnect the cable from the chassis USB connector.

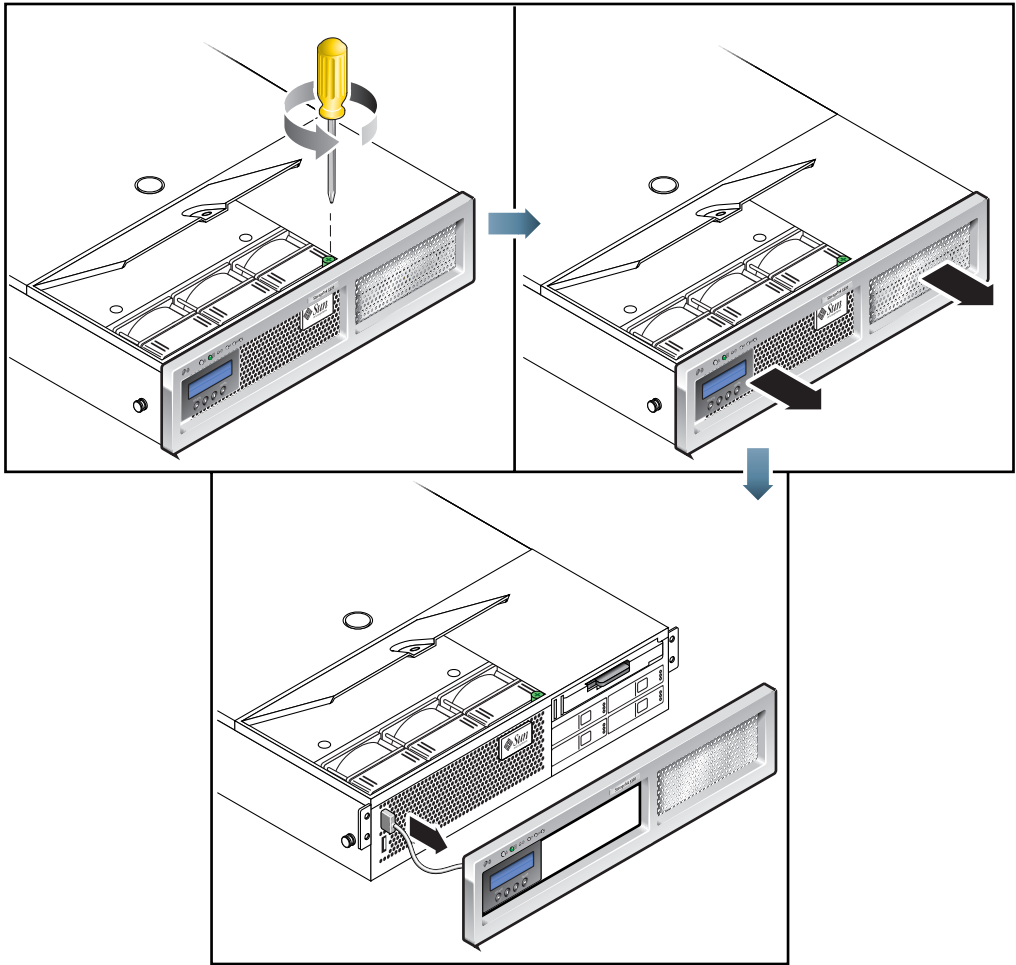


FIGURE 12-3 Removing the Front Bezel



Caution: When the front bezel is removed, the flash disk is accessible. Never remove the flash disk while the server is powered on. The flash disk must be replaced by Sun field service, it is not a customer-replaceable unit.

Removing the Front Cover

1. Open the door to the fan bay. See [FIGURE 12-4](#).
2. While holding the fan bay door open, slide the front cover toward the front of the chassis approximately 0.25 inch (6 mm).
3. Raise the back edge of the cover and then lift it off of the chassis.

Note: When you replace the front cover, place the front edge on the chassis first, then set it down into the keyed slots on the chassis sides before sliding it back.

Note: When you remove any cover, the intrusion switch that is on the front I/O board automatically powers down the system to standby power mode.

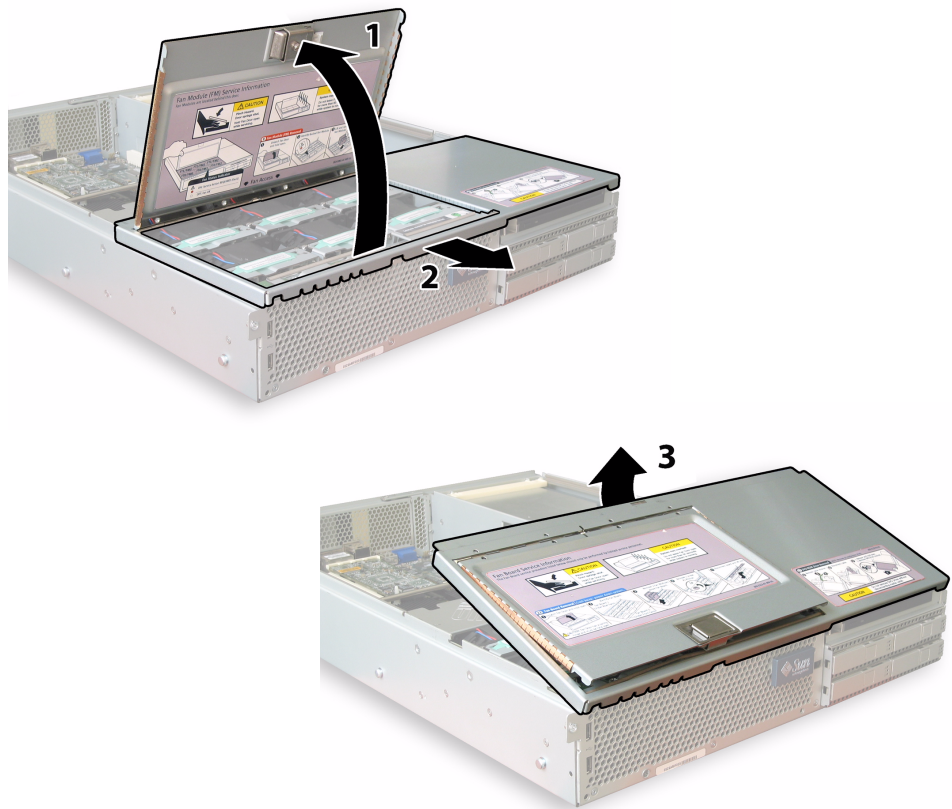


FIGURE 12-4 Removing the Front Cover

Locations of Customer-Replaceable Units

FIGURE 12-5 shows the locations of the customer-replaceable units (CRUs) that are documented in this section.

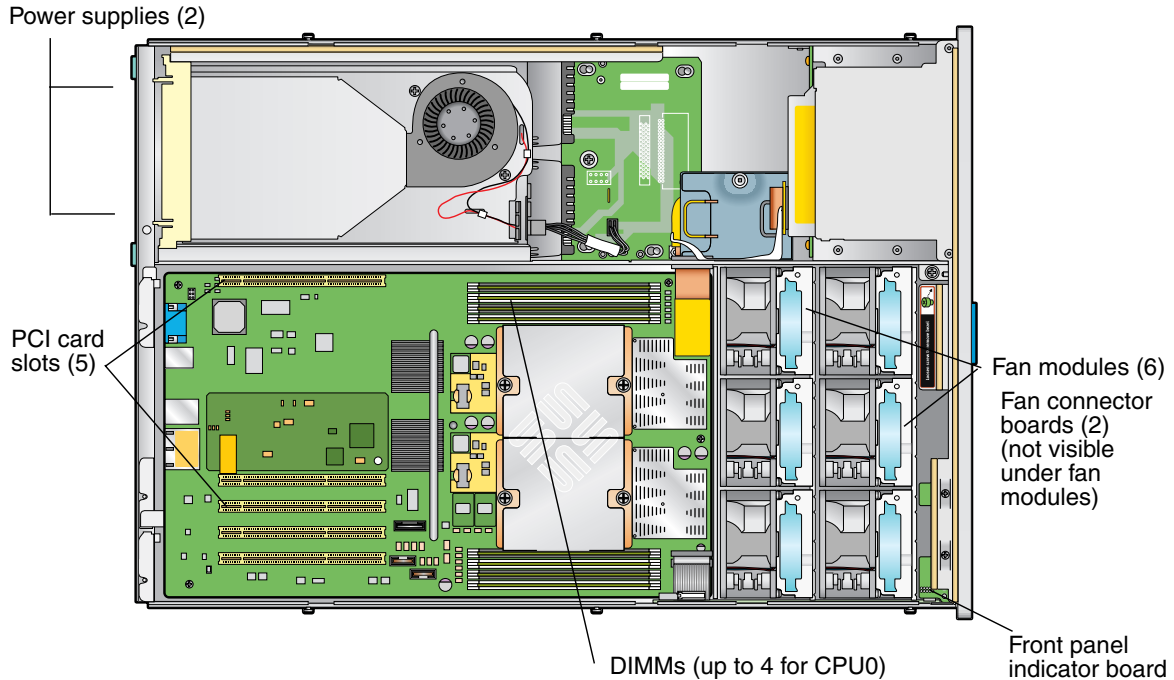


FIGURE 12-5 Replaceable Component Locations

Replacing Components

This section describes removal and replacement procedures for CRUs. Field-replaceable units (FRUs) must be replaced only by trained service technicians. Contact Sun Services for assistance with FRU replacements.

This section contains procedures for replacing the following CRUs:

- [“Replacing a Fan Connector Board” on page 225](#)
- [“Replacing the Front Panel Indicator Board” on page 227](#)
- [“Replacing the Power Supply” on page 229](#)

- [“Replacing Memory Modules” on page 231](#)
- [“Replacing a Fan Module Assembly” on page 233](#)
- [“Replacing the Rear Fan Tray” on page 235](#)
- [“Replacing a PCI Card” on page 236](#)

Replacing a Fan Connector Board

Perform the following steps to remove and replace a fan connector board. There is one supported fan connector board, part number 501-6917.

Note: Supported part numbers are subject to change.

1. Power off the server as described in [“Powering Off” on page 218](#).
2. If the server is in a rack, slide it far enough out of the rack so that you can open the fan bay door.

If you cannot safely view and access the component in this way, remove the server completely from the rack.

3. Open the fan bay door and hold it open. See [FIGURE 12-6](#).

Caution: When you open the fan bay door, be careful to hold it open with one hand so that it does not spring shut and injure your fingers. Do not hold the fan bay door open for more than 60 seconds while the server is running to avoid overheating the server.



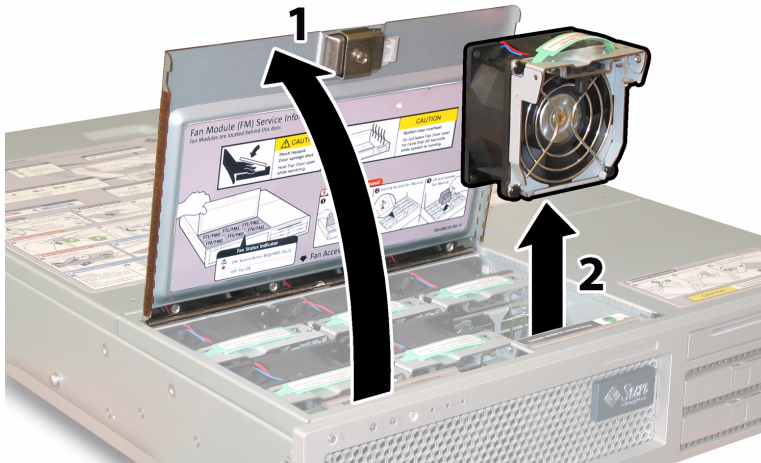


FIGURE 12-6 Opening the Fan Bay Door and Removing a Fan Module

4. Remove the three fan modules that are connected to the fan connector board that you are replacing.

Grasp each fan module by its plastic strap and lift it straight up out of the fan bay.

5. Remove the single screw that secures the fan connector board to the chassis, referring to [FIGURE 12-7](#). In that figure, the server is shown from the back with the front cover off and all fans removed to provide visibility. Do not remove the covers for this procedure.

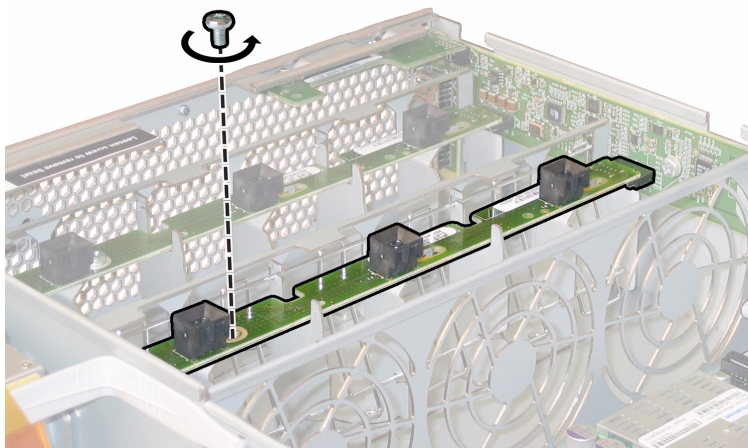


FIGURE 12-7 Removing the Fan Connector Board Securing Screw

- Slide the fan connector board toward the center of the chassis to disconnect it from the front I/O board and to release it from the two locating tabs on the chassis. See [FIGURE 12-8](#). In that figure, the server is shown from the back with the front cover off and all fans removed to provide visibility. Do not remove the covers for this procedure.

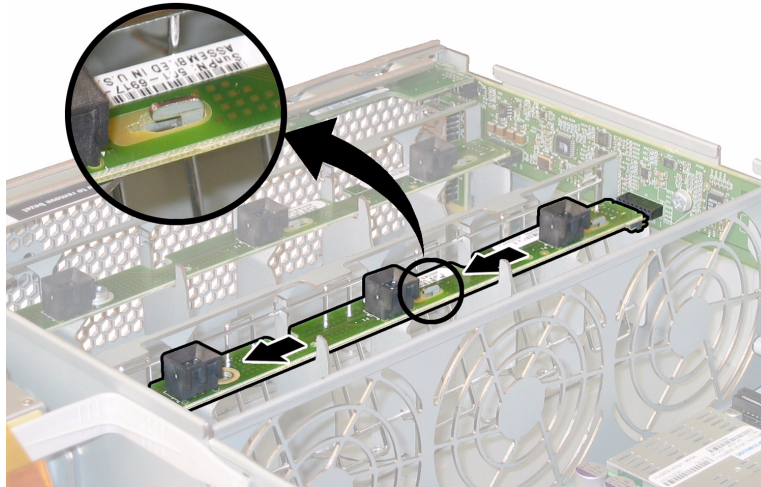


FIGURE 12-8 Releasing the Fan Connector Board

- Lift the board straight up to remove it from the system.
- Reverse the above steps to install a replacement fan connector board.

Replacing the Front Panel Indicator Board

Perform the following steps to remove and replace a front panel indicator board. There is one supported front panel indicator board, part number 501-6916.

Note: Supported part numbers are subject to change.

- Power off the server as described in [“Powering Off”](#) on page 218.
- If the server is in a rack, slide it far enough out of the rack so that you can remove the main cover and front cover.

If you cannot safely view and access the component in this way, remove the server completely from the rack.

3. Remove the main cover as described in [“Removing the Main Cover”](#) on page 220.
4. Remove the front bezel as described in [“Removing the Front Bezel”](#) on page 221.
Note: Always unfasten the bezel’s securing screw before removing the bezel.
5. Remove the front cover as described in [“Removing the Front Cover”](#) on page 223.
6. Remove the two screws that secure the front panel indicator board to the chassis.

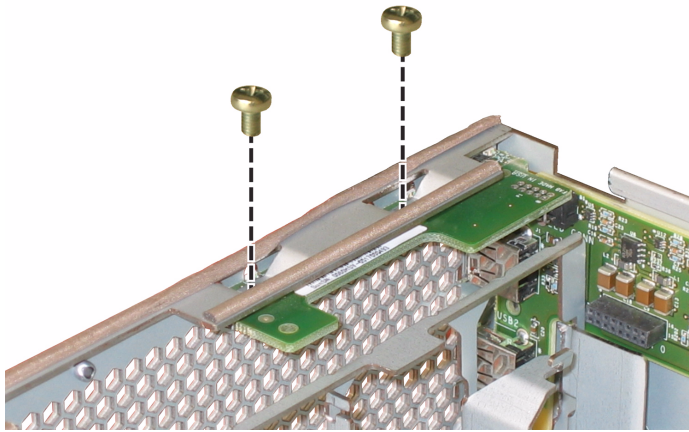


FIGURE 12-9 Removing the Front Panel Indicator Board Screws

7. While supporting the indicator board with your right hand, use your left hand to gently push the indicator board toward the center of the chassis to disconnect it from the front I/O board. See [FIGURE 12-10](#).

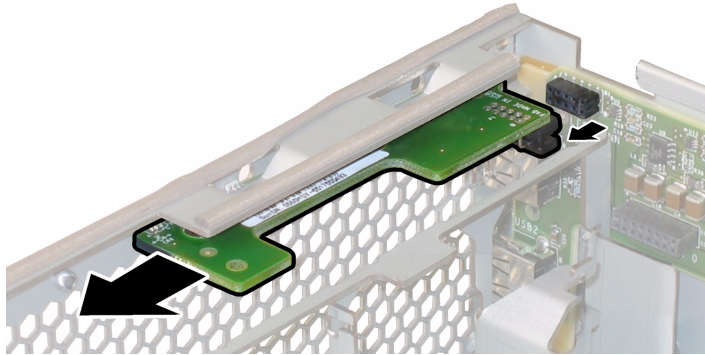


FIGURE 12-10 Removing the Front Panel Indicator Board

8. Remove the front panel indicator board from the chassis.
9. Reverse the above steps to install a replacement board.

Replacing the Power Supply

Perform the following steps to remove and replace a power supply. There is one supported power supply, part number 300-1757 (non-RoHS model) or 300-1945 (RoHS-compliant model).

Note: Supported part numbers are subject to change.

The internal system software designations of the two power supplies in the server are shown in [FIGURE 12-11](#).

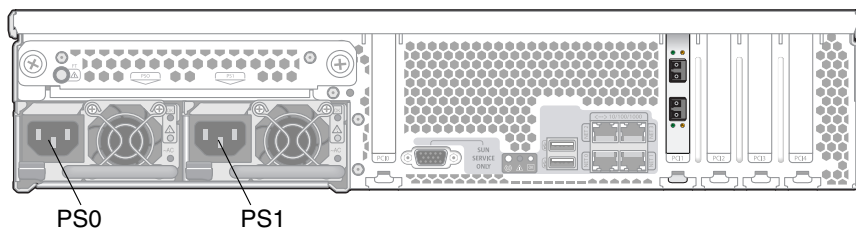


FIGURE 12-11 Designations of Power Supplies

1. Identify which power supply you will replace.

Each power supply has three LEDs that you can view from the back of the server:

- The top LED lights green to indicate that the power supply is operating properly.
- The middle LED lights amber to indicate that the power supply is faulty and must be replaced.
- The bottom LED lights green to indicate that the AC power source to the power supply is operating properly.

2. Disconnect the AC power cord from the power supply that you are replacing.

The power supplies are hot-swappable, so you do not have to shut down the server or disconnect the second power supply.

Note: The Service Action Required LEDs on the front panel and back panel blink when a power supply is unplugged. See [“Status Indicator LEDs” on page 322](#) for the LED descriptions.

3. Remove the power supply:

- a. Grasp the power supply handle and push the thumb latch toward the center of the power supply. See [FIGURE 12-12](#).
- b. While continuing to push on the latch, use the handle to remove the power supply from the chassis.



FIGURE 12-12 Removing a Power Supply

4. Reverse the above steps to install a replacement power supply. Press the new power supply into the bay until the thumb latch clicks, indicating that it is locked.

Replacing Memory Modules

Perform the steps detailed below to remove and replace the server's dual inline memory modules (DIMMs). There is one supported DIMM, part number 540-6453.

Note: Supported part numbers are subject to change.

The DIMM ejector LED can indicate a faulty DIMM. To view the fault LEDs in the ejector levers of the DIMM slots, put the server in standby power mode with the AC power cords attached. See [“Powering Off” on page 218](#). If the DIMM ejector LED is:

- Off: The DIMM is operating properly.
 - On (amber): The DIMM is faulty and must be replaced.
1. Review the following list of memory configuration guidelines before you remove or install any DIMMs:
 - The CPU can support a maximum of four DIMMs.
 - The DIMM slots are paired, and the DIMMs must be installed in pairs (0 and 1, 2 and 3). See [FIGURE 12-13](#). The memory sockets are colored black or white to indicate which slots are paired.
 - CPUs with only a single pair of DIMMs must have those DIMMs installed in that CPU's white DIMM slots (0 and 1).
 - Only PC3200 ECC and PC2700 ECC registered DIMMs are supported.
 - Each pair of DIMMs must be identical (same manufacturer, size, and speed).
 2. Power off the server as described in [“Powering Off” on page 218](#).
 3. If the server is in a rack, slide it far enough from out of the rack so that you can remove the main cover.

If you cannot safely view and access the component in this way, remove the server completely from the rack.
 4. Remove the main cover as described in [“Removing the Main Cover” on page 220](#).
 5. Locate the DIMM slot on the motherboard in which you will install or replace a DIMM. The internal system software designations of the DIMM slots are shown in [FIGURE 12-13](#).

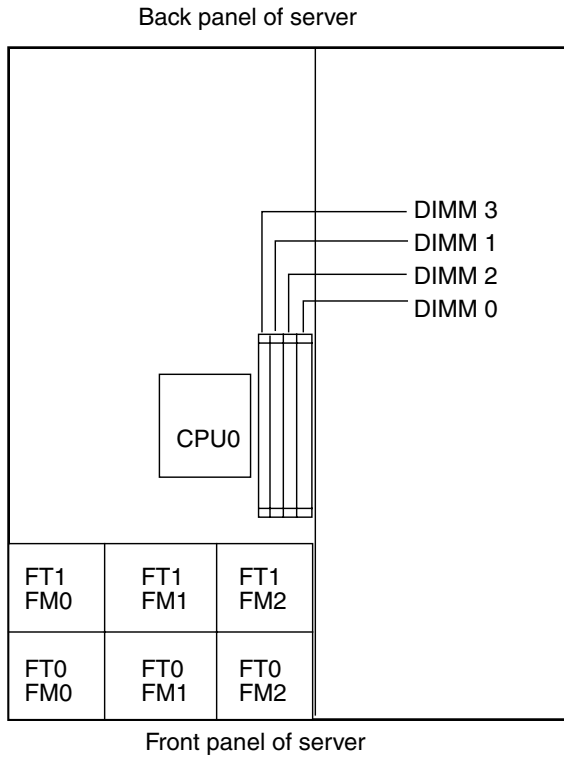


FIGURE 12-13 Designation of DIMM Slots

6. To remove a DIMM:
 - a. Rotate both DIMM slot ejectors outward as far as they will go. The DIMM is partially ejected from the socket. See [FIGURE 12-14](#).
 - b. Carefully lift the DIMM straight up to remove it from the socket.

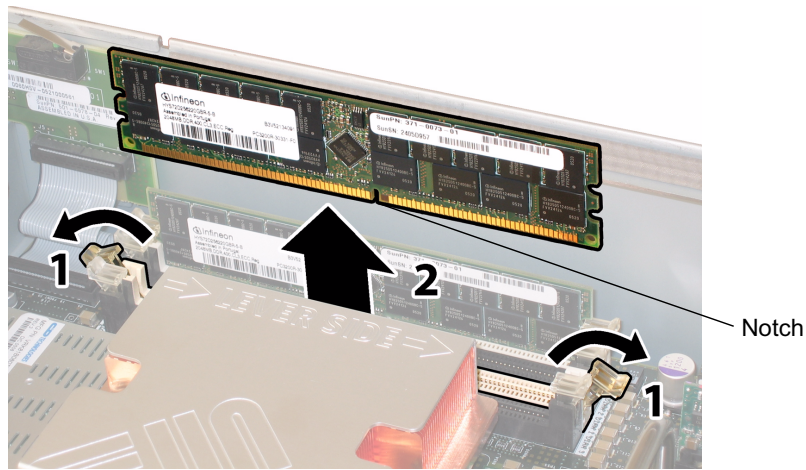


FIGURE 12-14 Removing a DIMM

7. To install a DIMM:

- a. Ensure that the DIMM slot ejectors at both ends of the memory socket are fully open (rotated outward) to accept the new DIMM.
- b. Align the notch in the bottom edge of the DIMM with the key in the DIMM socket. See [FIGURE 12-14](#).
- c. Press down evenly on both top corners of the DIMM until the ejectors snap over the cutouts at the left and right edges of the DIMM.

Replacing a Fan Module Assembly

Perform the following steps to remove and replace an individual fan module. There is one supported fan tray module, part number 541-0269.

Note: Supported part numbers are subject to change.



Caution: The fans are hot-swappable and can be removed and replaced while the system is running. Do not hold the fan bay door open for more than 60 seconds at a time to avoid overheating the server. Remove and replace only one fan at a time.

The internal system software designations of the fan connector boards, or fan trays (FTs), and fan modules (FMs) are shown in [FIGURE 12-15](#).

FT1 FM0	FT1 FM1	FT1 FM2
FT0 FM0	FT0 FM1	FT0 FM2

FIGURE 12-15 Fan Connector Boards and Fan Modules Viewed from Front of Server

1. If the server is in a rack, slide it far enough out of the rack so that you can open the fan bay door.

If you cannot safely view and access the component in this way, remove the server completely from the rack.

2. Open the door to the fan bay and identify the defective fan modules by inspecting the LEDs.

- Lit: The fan module is faulty and must be replaced.
- Off: The fan module is operating properly.

Caution: When you open the fan bay door, be careful to hold it open with one hand so that it does not spring shut and injure your fingers. Do not hold the fan bay door open for more than 60 seconds while the server is running to avoid overheating the server.

3. While holding the fan bay door open, grasp the faulty fan module by its plastic strap and lift it straight up out of the fan bay. See [FIGURE 12-16](#).

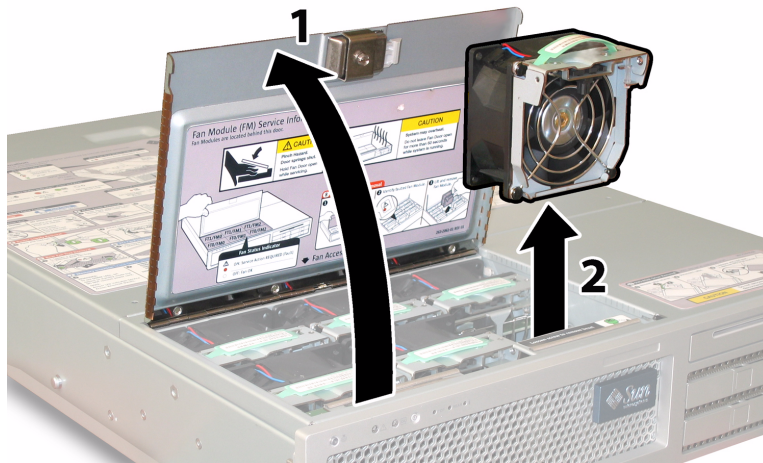


FIGURE 12-16 Opening the Fan Bay Door and Removing a Fan Module

4. Reverse the above steps to install a replacement fan module assembly.

Replacing the Rear Fan Tray

Perform the following steps to remove and replace the rear fan tray (blower tray). There is one supported blower tray, part number 541-0645.

Note: Supported part numbers are subject to change.

1. Working from the back of the server, unfasten the two captive thumbscrews on the face of the rear fan tray. See [FIGURE 12-17](#).

The internal system software designation of the rear fan tray is `I/O FAN`. The rear fan tray has one fault LED on its face, indicating the following:

- Off: The fan tray is operating properly.
- On (amber): The fan tray is faulty and must be replaced.

2. Remove the rear fan tray from the chassis.

The fan tray cable connector disengages from the internal connector on the chassis, as illustrated in [FIGURE 12-17](#). In that figure, the server is shown with the cover in order to make the component visible; do not remove the cover for this procedure.

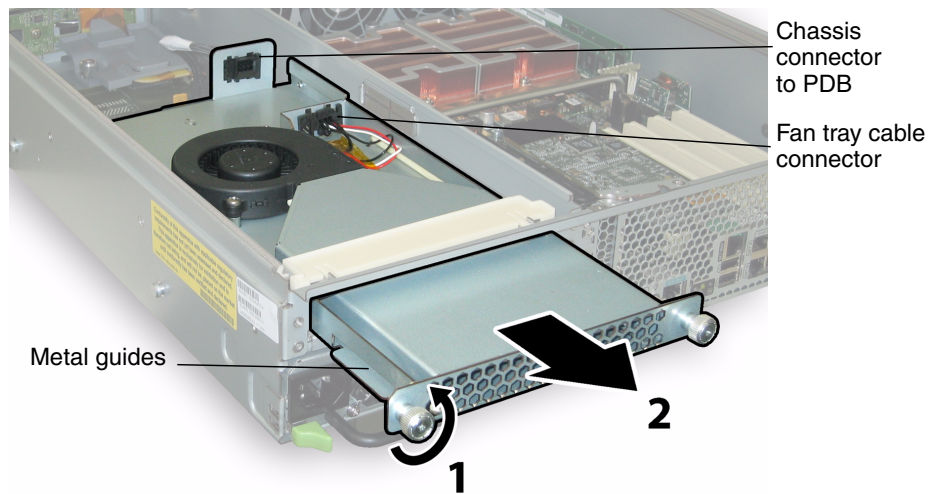


FIGURE 12-17 Removing the Rear Fan Tray

3. Reverse the above steps to install a replacement rear fan tray. Make sure the metal guides on the fan tray sides (see [FIGURE 12-17](#)) engage the plastic rails inside the chassis bay evenly.

Replacing a PCI Card

Perform the following steps to remove and replace a PCI card.

[TABLE 12-1](#) lists the supported part numbers for this component.

Note: Supported part numbers are subject to change.

TABLE 12-1 Supported PCI Card Part Numbers

Component	Part Number
Dual-Port Fibre Channel	375-3421
Single-Port U320 SCSI HBA	375-3366
NIC Dual-Port Fibre	375-3250
NIC Dual-Port Cu	370-6687

1. Power off the server as described in [“Powering Off” on page 218](#).
2. If the server is in a rack, slide it far enough out of the rack so that you can remove the main cover.

If you cannot safely view and access the component in this way, remove the server completely from the rack.
3. Remove the main cover as described in [“Removing the Main Cover” on page 220](#).
4. Locate the PCI card slot in which you will install or replace a PCI card.

The internal system software designations and the speeds of the five PCI slots are shown in [FIGURE 12-18](#). The slots for the PCI-X cards are detected by the system BIOS during bootup in this order: 0, 2, 3, 4, 1.

Note: Before you install a card, consult the manufacturer's documentation for system requirements and configuration information for your specific PCI card.

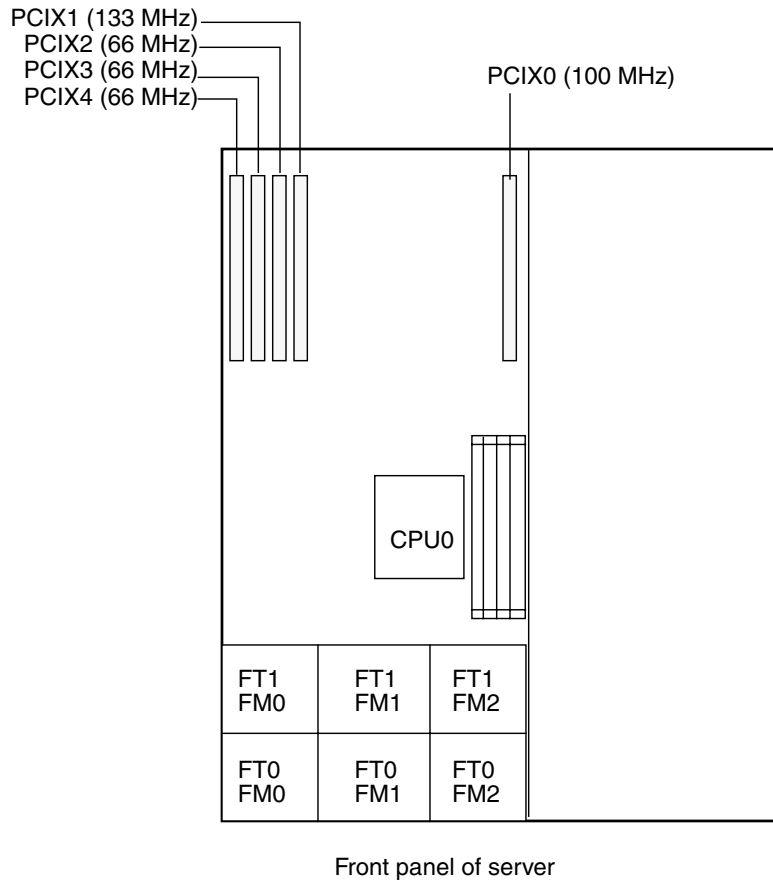


FIGURE 12-18 PCI Slot Designations and Speeds

5. Remove any existing PCI card from the slot:
 - a. Disconnect any external cables that are attached to the PCI card.
 - b. Working from the back of the chassis, pivot open the PCI card latch that covers the PCI card's back connector panel. See [FIGURE 12-19](#).

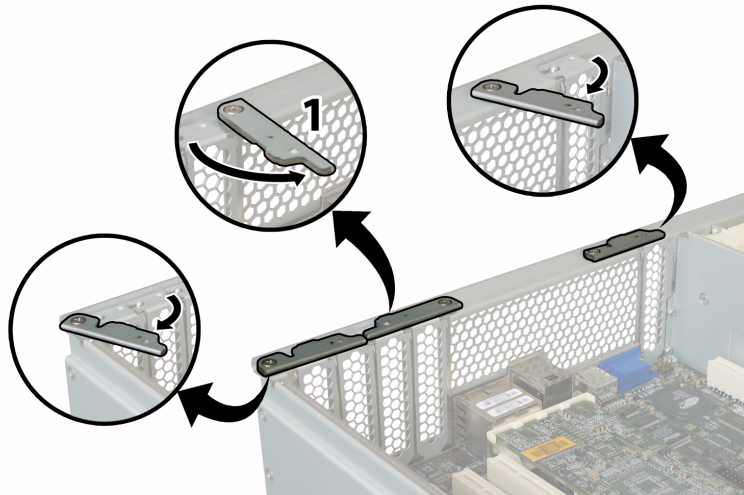


FIGURE 12-19 Opening a PCI Card Securing Latch

- c. Pull the PCI card out of the PCI slot. Ensure that the PCI card's back connector panel is released from the tab on the chassis back panel.
- 6. If there is no PCI card in the slot, remove the PCI-card filler panel from the chassis back panel. See [FIGURE 12-20](#).

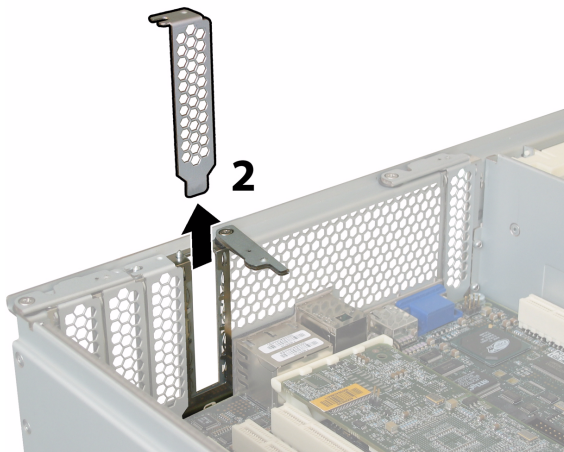


FIGURE 12-20 Removing a PCI-Card Filler Panel

- 7. Install a PCI card:
 - a. Working from the back of the chassis, pivot the PCI card latch for the slot open to receive the new PCI card. See [FIGURE 12-19](#).

- b. Insert the PCI card into the PCI card slot. Ensure that the PCI card's back connector panel engages the tab in the chassis back panel. See [FIGURE 12-21](#).

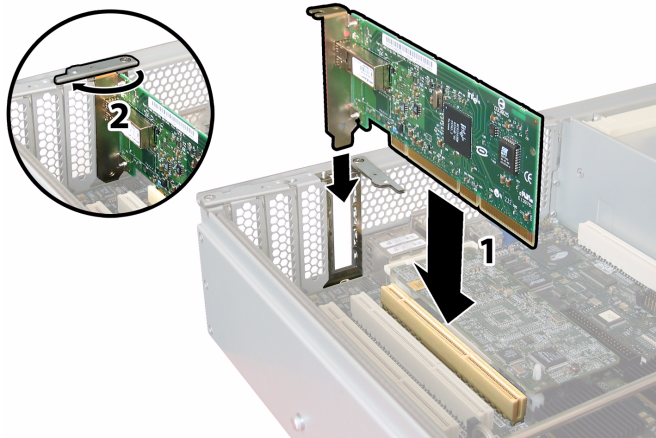


FIGURE 12-21 Installing a PCI Card

- c. Pivot the PCI card latch closed over the back connector panel of the PCI card until it locks. See [FIGURE 12-21](#).

Console Administration

The administrator console is an alternative to using the Web Administrator graphical user interface (GUI) for managing the NAS appliance or gateway system. You can use a number of protocols, such as Telnet, SSH, and RLogin to connect to the console, as long as the application you use has an ANSI-compatible terminal emulator. This appendix uses Telnet, because it is readily available in the Windows operating system.

Note: Avoid simultaneous updates by Telnet/CLI and Web Administrator users.

This appendix includes the following sections:

- [“Accessing the Administrator Console” on page 242](#)
- [“System Management” on page 244](#)
- [“Managing Routes” on page 249](#)
- [“Name Services” on page 250](#)
- [“Managing the Server File System” on page 253](#)
- [“Shares and Quotas” on page 256](#)
- [“Security” on page 261](#)
- [“Mirroring File Volumes” on page 271](#)
- [“Monitoring” on page 281](#)
- [“Configuring the NAS for iSCSI” on page 288](#)
- [“System Maintenance” on page 292](#)

Accessing the Administrator Console

This section describes how to access and get started with the administrator console, as follows:

- [“Opening a telnet Session” on page 242](#) tells how to log in through Telnet.
- [“Console Menu Basics” on page 243](#) describes the basics of working from the administrator console’s main menu.
- [“Viewing Man Pages” on page 244](#) tells how to display man pages for the console commands.

The examples shown here use Windows Telnet to access the administrator console; however, you can use any protocol that has an ANSI-compatible terminal emulator.

Opening a telnet Session

Use the following procedure to control the NAS server through an ANSI-compatible terminal emulator. This procedure uses Windows Telnet as an example.

Note: You might have to alter the remote access security settings to enable access to the command-line interface. For details, see [“Setting Remote Access Options” on page 171](#).

1. Click Start > Run from your Windows desktop.
2. In the Run window, type `cmd` and click OK.
3. At the command prompt, type the following command and press Enter:

```
telnet ip-address,
```

where *ip-address* is the IP address of the server.

4. If administrative access is password-protected, enter the password. The following prompt is displayed:

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

5. Press Enter to display the console menu. See [“Console Menu Basics” on page 243](#).

To display the command line, type `admin` and then type the administrator password, if prompted. See [“Viewing Man Pages” on page 244](#) for an index of commands.

When using administrator console, you can press the Esc key at any time to display the prompt.

When using the command line, you can enter menu to display the administration console.

Console Menu Basics

The main console menu consists of the following sections:

- **Operations** – Choose any number to perform the corresponding server operation.
- **Configurations** – Choose any letter to perform the corresponding server configuration command.
- **Access Control** – Choose any letter to set up access to the corresponding menu items.
- **Extensions** – Choose any letter to identify the corresponding extension. Use the spacebar to scroll through the extensions list.
- **Instructions box** – The box at the bottom of every screen displays the tasks you can perform, the letter to choose to perform each action, and numbers/ letters to choose to make field selections.

To use the console menu:

1. Choose the menu item by entering the corresponding letter or number. For example, type **1** to choose Activity Monitor.
2. Press the spacebar to scroll through a list, for example, to view more options under the Extensions heading.
3. Press Enter or Tab to move to the next field, if the cursor does not advance.
4. Use the following keys to edit screen fields:

TABLE A-1 Console Menu Keyboard Functions

Keys	Action
Backspace, Delete, Ctrl+H	Deletes the previous character.
Ctrl+U	Deletes the entire field.
Enter, Ctrl+M, Ctrl+J, Ctrl+I, Tab	Completes the current entry and moves the cursor to the next field.
Esc	Returns to the menu without saving any changes.

Viewing Man Pages

You can view man pages from the command line. Enter the man command, followed by the name of the command, for example ads :

```
falcon125> man ads
```

You can also access the man pages using a web browser, using this URL:

```
http://host-name/man
```

Both operations display an index of man pages. Click a command to display the content for that command.

System Management

You can use the console administrator to perform system management tasks. This section describes the following tasks:

- ["Configuring TCP/IP" on page 244](#)
- ["Modifying the Administrator Password" on page 245](#)
- ["Setting the Time and Date" on page 245](#)
- ["Setting Time Synchronization" on page 246](#)
- ["Enabling Antivirus Protection" on page 248](#)
- ["Selecting a Language" on page 249](#)

Configuring TCP/IP

To configure TCP/IP:

1. From the Configuration menu, choose Host Name & Network.
2. Choose 1, Edit fields.
3. Enter the server host name.
4. For the first NIC port, enter the Maximum Transfer Unit (MTU) or press Enter to use the default.
5. Enter the IP address for the NAS server.

6. Enter the IP subnet mask for the NAS server.
7. Enter the broadcast IP address, which specifies the IP address used to send broadcast messages to the subnet.
8. If the cursor stops on the IP Alias Info field, specify an alias IP address for the port. Choose 1, Setup, to configure one or more alias IP addresses.

Aliases are used to specify the IP addresses of obsolete systems that have been replaced by NAS storage.

You can have up to nine aliases per interface for single-server systems and up to four aliases for dual-server systems. To remove an alias from the list, delete its address. Changes are not saved until you click Apply.
9. Repeat [Step 3](#) through [Step 8](#) for each port, using the spacebar to scroll down if more than three ports are present.
10. Enter the gateway address.
11. Choose 7, Save changes.

Modifying the Administrator Password

To modify the administrator password:

1. From the Access Control menu, choose Admin Access.
2. Select Y (yes) to enable password protection, or N (no) to disable it.
Note: Always protect your system with a password.
3. If you select Yes, the system prompts you for a password. Enter the password and then enter it again to confirm.
4. Choose 7, Save changes to activate the new password.

In a cluster configuration, changes made to the administrator password on one server are propagated immediately to the other server.

Setting 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: After the secure clock has been initialized, it cannot be reset. Therefore, it is important that you set the time and date accurately.

To set the time zone, time, and date:

1. From the Configuration menu, choose Timezone, Time, Date.
2. Select the appropriate time zone and press Enter.
3. Enter the new date.

The format is YYYYMMDD, where YYYY is the year, MM is the month, and DD is the day. For example, 20070501 equals May 1, 2007.

4. Enter the current time, using a 24-hour clock (*hh:mm*).
5. Choose 7, Save changes.

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

Setting Time Synchronization

You can configure the system to synchronize its time with either an NTP or 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. With the NAS OS, you can configure up to two NTP servers.
- RDATE servers are normally present on Unix systems and enable you to synchronize system server time with RDATE server time.

These options are discussed separately below.

Setting UP NTP for Time Synchronization

Follow these steps to synchronize the clocks of computers to a reference time source using NTP:

1. From the Extensions menu, choose NTP Configuration.
2. Choose 1, Edit fields to configure NTP settings.
3. Select Y (yes) to enable NTP.
4. Select Y (yes) to enable the first NTP server.
5. Enter the name or IP address of the first NTP server the appliance or gateway system polls for the current time.
6. Select the type of Authentication to use, either 0 (none) or 1 ((symmetric-key).

Symmetric key authentication support lets the appliance or gateway system verify that the NTP server is known and trusted by using a key and key ID. The NTP server, and the appliance or gateway system, must agree on the key and key ID to authenticate their messages.
7. If you select Symmetric Key as the authorization scheme in the previous field, enter the Key ID associated with the private key from the key file to be used with this NTP server.

The valid range for this value is 1 to 65534.
8. To configure a second NTP server, repeat [Step 4](#) through [Step 7](#) for Server 2.
9. In the Min. Polling Interval field, type the minimum polling rate for NTP messages.

This value, raised to the power of two, is the minimum number of seconds of the polling interval. For example, entering 4 results in 16 seconds between polls. The valid range for this field is 4 to 17.
10. In the Max. Polling Interval field, type the maximum polling rate for NTP messages.

This value, raised to the power of two, is the maximum number of seconds of the polling interval. For example, entering 4 results in 16 seconds between polls. The valid range for this field is 4 to 17, but must be larger than the minimum polling interval.
11. In the Broadcast Client Enabled field, select Y (yes) for the appliance or gateway system to respond to server broadcast messages received on any interface.
12. In the Require Server authentication field, select Y (yes) to require authentication for servers using the Broadcast client.

NTP servers not using authentication will not be accepted.
13. Choose 7, Save changes.

Setting Up the RDATE Server and Tolerance Window for Time Synchronization

To set up the RDATE server and tolerance window:

1. From the Extensions menu, choose RDATE time update.
2. Choose 1, Edit fields.
3. Enter the RDATE server name or IP address.
4. Enter the tolerance.

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

5. Choose 7, Save changes.

Enabling Antivirus Protection

If you have an antivirus scan engine running on your network, you can configure antivirus protection on the system. For more detail about antivirus protection, see ["About Virus Scanning" on page 71](#).

To enable antivirus protection:

1. From the Extensions menu, choose Anti-Virus Configuration.
2. Choose 1, Edit fields.
3. In the AVA Enable field, specify Y (yes) to enable antivirus protection.
4. In the Max Scan Size field, enter 1 to 1023 and KB, MB, or GB.
5. In the Access field, enter the action (Allow or Deny) to be taken if a file exceeds the maximum scan size.
6. For each of up to four scan-engine systems:
 - a. Specify the Internet Protocol (IP) address of the system that is running the scan engine software you want to use.
 - b. Identify the port on the scan-engine system, through which the scan engine listens for scan requests. This is typically port 1344.

- c. Specify the maximum number of concurrent file scan operations (connections) the scan engine can handle from the NAS device. The default is two operations.

7. Choose 7, Save Changes.

To specify which file types are included or excluded from the virus scan, use the CLI command `vscan`. See the manpage for details.

Selecting a Language

You can specify the language for NFS and CIFS.

To select a language:

1. From the Extensions menu, choose Language Selection.
2. Enter the desired language.

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, choose Host Name & Network.
2. Choose 2, Manage Routes.
3. Choose 1, Add route, then choose 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.
6. Enter the path or gateway address used to connect the NAS appliance or gateway system with its destination. A gateway device must connect to the same subnet as the NAS appliance or gateway system.

7. Choose 7, Save Changes.

Name Services

The name, services, and functions available through the console interface vary from those available through the Web Administrator.

Setting Up DNS, Remote Log, and Local Log

The domain name system (DNS) is a hierarchical name system that translates domain names into IP addresses. Remote logging uses the `syslogd` utility to send all log messages to the specified server, creating a centralized record of all events from all servers into one log. You can enable remote logging only if you have a Unix system with the `syslogd` utility on the network that can receive the NAS system log. If you do not set up remote logging, set up the local log

To set up DNS, Dynamic DNS, remote logging or local logging:

1. From the Configuration menu, choose DNS & SYSLOGD.
2. Choose 1, Edit fields.
3. Select Y (yes) to enable DNS.
4. Enter the IP address for the DNS server to be consulted first for name resolution.
5. Enter the IP address of the server to be consulted second for name resolution.
If you do not have a secondary DNS server, leave this field blank.
6. Enter the domain name of the DNS server.
7. Enter the maximum number of times the system attempts a DNS query for each DNS server.
8. Enter the number of seconds of delay between attempts to query each DNS server.
9. Select Y (yes) to enable Dynamic DNS updates, which enable non-secure dynamic updates to occur during bootup. If you leave this as No, skip to [Step 12](#)

10. To enable secure updates, enter the name of a Windows user with whom the dynamic DNS client can verify updates. This user must have administrator rights.
11. Enter the password of the Dynamic DNS user.
12. Select Y (yes) to enable remote logging, which requests that the NAS appliance or gateway system send log messages to a remote `syslogd` server.
If there is no `syslogd` server on the network, select N (no) and skip to [Step 16](#)
13. Enter the `syslogd` server name or IP address.
14. Select the facility code that will be assigned to all NAS messages that are sent to the remote log, then press Enter.
15. For each type of system event you want to send to the log, type Y (yes) when prompted. Press Enter to move to the next event type without changing the setting. Each event type represents a different priority, or severity level, as described under "[About System Events](#)" on page 159.:
16. Type Y (yes) to enable local logging.
17. Type the log file path (directory) and file name in the Log File field.
Note: You cannot set up local logging to either the `/cvol` or `/dvol` directory.
18. Type the maximum number of archive files in the Archives field. The range is from 1 to 9.
19. Type the maximum file size in kilobytes for each archive file in the Archives field. The range is from 1000 to 999,999 kilobytes.
20. Choose 7, Save changes.

Setting Up a Name Service

To enable NIS or NIS+:

1. From the Configuration menu, choose NIS & NIS+.
2. Choose 1, Edit fields.
3. Select Y (yes) to enable the NAS appliance or gateway system to periodically update its hosts, users, and groups files through an NIS server.
4. Enter the NIS domain name.
5. Enter the NIS server name or IP address.

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.
11. Select Y (yes) to enable NIS+ for the NAS appliance or gateway system.
12. Enter the NIS+ home domain server address.
13. Enter the NIS+ home domain name.
14. Enter the secure RPC password for the NIS+ server.
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.
16. Choose 7, Save changes.

After NIS is set up, 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.

Setting Lookup Order for Name Service

You can specify which service is used first for user, group, and host lookup functions.

To set up lookup orders:

1. From the Configuration menu, choose Lookup orders.
2. Choose 1, Edit fields.
3. Select the order for resolving user information (between NIS and NIS+) and press Enter.
4. Select the order for resolving group information (between NIS and NIS+) and press Enter.
5. Select the first, second, third, and last services for resolving host information, then press Enter.

6. Choose 7, Save changes.

Managing the Server File System

There are several procedures available through the console that let you manage the Server File System (SFS) volumes. The most common are described in the following sections:

- ["Configuring Drive Letters" on page 253](#)
- ["Creating a New Disk Volume" on page 254](#)
- ["Renaming a Partition" on page 254](#)
- ["Adding an Extension Segment" on page 255](#)
- ["Deleting a Disk Volume" on page 255](#)

Configuring Drive Letters

Drive letters are assigned to file volumes available for sharing through SMB/CIFS. You can assign the drive letter mappings through the console, except for drive C:, which can only be assigned to `\cvol`. If no drive letters are available, the file system is created but the following log message is displayed:

```
No drive letter available
```

To assign a drive letter to the new file system, you must reassign an existing drive letter.

To manually reassign a drive letter to a file volume:

1. From the Configuration menu, choose Drive Letters.
2. Enter the drive letter you want to change.
3. Enter the file volume name you want to assign to the new drive letter.
You can only assign existing file volumes to drive letters.
4. Press Esc to exit this screen.

Creating a New Disk Volume

To create a new disk volume:

1. From the Configuration menu, choose Disks & Volumes.
2. Type the letter of the drive you want to configure.
3. Choose 1, Edit.
4. Choose 1, Create partition.
5. Select the partition type for the drive.

Press Enter to accept the default (for example, `sfs2` for the primary volume, or `sfs2ext` for a segment).

6. Enter the disk volume label.
7. If the system asks whether you want to enable Compliance Archiving on this volume and you have a license for the Compliance Archiving Software, type Y to create a compliance-enabled volume.

Note: Gateway configurations support advisory compliance but not mandatory compliance.

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



8. Enter the disk volume size in megabytes (MB).
9. Choose 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 at the main console menu.

Renaming a Partition

If you attempt to rename a volume during a write operation, CIFS and NFS clients behave differently. If you attempt to rename a Windows volume during a write operation, CIFS I/O stops after the volume is renamed. For NFS shares, I/O will continue after you rename a Unix volume.

To rename a partition:

1. From the Configuration menu, choose Disks & Volumes.
2. Type the letter of the drive you want to rename.
3. Choose 1, Edit.
4. Choose 3, Rename.
5. Enter the new name for the partition.

Note: Strict compliance-enabled volumes cannot be renamed.

Adding an Extension Segment

To add an extension, you must first create an `sfs2ext` partition on that volume.

Note: After the extension volume is attached to the `sfs` file volume, it cannot be detached. This is an irreversible operation. The only way to separate them is to delete the `sfs` file volume.

To add an extension:

1. From the Configuration menu, choose Disks & Volumes.
2. Type 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. Choose 5, Segments.
5. Choose 1, Add an extension segment.
6. Select the letter next to the extension drive you want.
7. Choose 7, Proceed.

Deleting a Disk Volume

Note: Strict compliance-enabled volumes cannot be deleted.



Caution: All data in the volume is lost when you delete a volume.

To delete a disk volume:

1. From the Configuration menu, choose Disks & Volumes.
2. Type the letter of the drive you want to configure. If you have more than 26 disk drives (disk volumes), press the spacebar to scan through them.
3. Choose 1, Edit.
4. Choose 8, Delete.
5. Enter the disk volume name.
6. Choose 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 at the main console menu.

Shares and Quotas

You can manage shares and quotas using the console.

SMB/CIFS Shares

Common Internet File System (CIFS) is a Windows file-sharing service that uses the Server Message Block (SMB) protocol. CIFS provides a mechanism for Windows client systems to access files on the NAS appliance or gateway system.

Setting Up SMB/CIFS Shares

To set up shares:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose A, Domain Configuration.
3. Type a workgroup or domain name in the Domain field.
4. Define the domain scope, if applicable.

5. Type a text description of the appliance or gateway-system server.
6. Type 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, specify the administrative user name and password.
10. Choose 7, Save changes.
If you changed the security mode between Secure Share Level and NT Domain Auto UID, the NAS appliance or gateway system 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`, the autohome path must 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 log-in name.

If the feature is disabled, the autohome path parameter is not relevant and will not be validated.

If the feature is enabled and the path is a zero length string, the configuration will be ignored. Otherwise, the path will be validated. If the autohome path parameter does not represent an existing directory path, an informational message will be written to the system log. For example, if the specified base path was `/vol1/home`, the log message would be as follows:

```
SMB autohome: /vol1/home: no such directory
```

The log message is intended to inform the system administrator of the situation, but the configuration is still considered valid. The system will operate normally, but autohome shares will not be created. If the directory path is created at some later time, autohome shares will be added and removed, as required, from that point on.

To enable autohome shares:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose F, Autohome Setup.
3. Choose 1, Edit fields.
4. Select Y (yes) to enable autohome shares.
5. Type 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 log-in name.

6. Choose 7, Save changes.

Adding a Share

After the Server Message Block (SMB) Common Internet File System (CIFS) set up is complete, you must define SMB/CIFS shares. Shares allow Windows users to access directories in the NAS appliance or gateway system.

To add a share:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose E, Shares.
3. Choose 8, Add a share.
4. Type the share name. This is the name that users will see on the network. The share name can be up to 15 characters in length, and can include any alphanumeric characters except those listed below:
" / \ [] : | < > + ; , ? * =
5. Type the path to the volume, and optionally the directory, you wish to share.
6. Type a comment about this directory, if desired.

7. If Active Directory Service (ADS) is enabled for the share, as described under ["Configuring Windows Security" on page 28](#), specify the location in the ADS directory where the share will be published.

Type the container information following LDAP DN (Lightweight Directory Access Protocol, distinguished name) notation. Objects, such as users and shares, are located in Active Directory domains according to a hierarchical path, which includes each level of "container" objects.

Type the path in terms of the cn (common name) folder or ou (organizational unit) of the share. Do not include the domain name in the path. The cn containers are default folders in the root folder. All other containers are ou folders. For example, if the share will reside in a shares organizational folder within an organizational parent folder called accounting, you would type the following:

```
ou=shares,ou=accounting
```

8. If your system is configured for Windows Workgroup mode, as described under ["Configuring Windows Security" on page 28](#):

- From the Password Protection drop-down menu, select Yes or No.
- If you select Yes above, type the password for Windows Workgroup users who will have read/write access to the share.
- Also if you select Yes above, type the password for Windows Workgroup users who will have read-only access to the share.
- Type the user identification (UID) of the user accessing the specified path through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.

Together with the Group ID field, the UID provides the sole means of security for NAS file ownership and access by Windows Workgroup users.

- Type the group identification (GID) of the user accessing the specified path through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.
- Type the three-digit Umask to specify access permissions for the share. For detailed information about access permissions for shares, see ["About Share Access Permissions" on page 115](#).

9. Choose 7, Save changes.

Editing a Share

To edit a share:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose E, Shares.
3. Type the letter corresponding to the share you are editing.
4. Choose 1, Edit fields.
5. Modify the share name (as the new share name), and any of the other information shown. See [“Adding a Share” on page 258](#) for field details.
6. Choose 7, Save changes.

Deleting a Share

To delete a share:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose E, Shares.
3. Type the letter corresponding to the share you wish to delete.
4. Choose 8, Delete.

Setting Up Active Directory Service

When the Active Directory Service (ADS) is enabled and set up, the NAS appliance or gateway system performs ADS updates.

To enable ADS service:

1. From the Extensions menu, choose ADS Setup.
2. Choose 1, Edit fields.
3. Select Y (yes) to let the ADS client publish the appliance or gateway system shares to ADS.
4. Type the Windows domain on which ADS is running. The NAS appliance or gateway system must also belong to this domain.
5. Type the name of a Windows user with administrative rights. The ADS client verifies secure ADS updates with this user.
6. Type the Windows administrative user’s password.

7. In the User Container field, specify the ADS path for the Windows administrative user in LDAP DN notation. For more information see ["Enabling ADS" on page 87](#).
8. If the ADS domain uses sites, specify the appropriate site name in the Site field. Otherwise, leave the Site field blank. If specified, the Site will be included when selecting a domain controller.
9. Type, in uppercase letters, the Kerberos realm name used to identify ADS. This is normally the ADS domain.
10. Type 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. Choose 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, choose Disks & Volumes.
2. Select the drive for which you are enabling quotas.
3. Choose 1, Edit.
4. Choose 4, Quotas on/off.
5. Choose 1, Turn quotas on or 8, Turn quotas off.

Security

You can set up groups and credential mapping to ensure security. The tasks are described in the following sections:

- ["Configuring User Groups" on page 262](#)

- ["Modifying Group Privileges" on page 263](#)
 - ["User and Group Maps" on page 264](#)
 - ["Mapping and Securable Objects" on page 266](#)
 - ["Configuring the Host List" on page 268](#)
 - ["Managing Trusted Hosts" on page 269](#)
 - ["Managing Volume Access for NFS Clients" on page 270](#)
 - ["Locking and Unlocking the Console" on page 270](#)
-

Configuring User Groups

This section describes how to configure NAS user groups. The requirements for built-in local groups are different from those of a Windows NT system. For a complete description of user groups, see ["About Local Groups" on page 94](#).

Note: In a cluster configuration, changes made to user groups on one server are propagated immediately to the other server.

Adding a Group

To add a group:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose B, Local Groups.
3. Choose 8, Add a Group to add a local group.
4. Enter in the name of the group.
5. Enter a description of the group, if applicable.
6. Choose 7, Save Changes to save the new group.

Adding a Member to a Group

To add a member to a group:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose B, Local Groups.

3. Select the letter of the group you want to modify.
4. Choose 2, Members to change the membership of the group.
5. Choose 8, Add to add a member.
6. Type in the domain and user name in the following format: *domain\username*
The domain identifies the domain where the user name can be authenticated. For example, typing `BENCHLAB\john` identifies the domain `BENCHLAB` where the user `john` can be authenticated.
7. Press Enter.
8. Choose 7, Save Changes to save the new member.

Removing a Member From a Group

To remove a member from a group:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose B, Local Groups.
3. Select the letter of the group you want to modify.
4. Choose 2, Members to change the membership of the group.
5. Select the letter corresponding to the group member you want to remove.
6. Select Y in response to the prompt.

Modifying Group Privileges

Follow the steps below to modify local group privileges. For a description of user group privileges, see ["About Configuring Privileges for Local Groups" on page 94](#).

Note: In a cluster configuration, changes made to user privileges on one server are propagated immediately to the other server.

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose B, Local Groups.
3. Select the letter of the group you want to modify.
4. Choose 3, Privileges to change the privileges of the group members.

5. Select the letter of the privilege that you want to add or remove.
6. Choose 7, Save Changes to save the changes that you made.

User and Group Maps

For a complete description of user and group credentials, see ["About Mapping User and Group Credentials" on page 102](#).

Note: In a cluster configuration, changes made to user and group maps on one server are propagated immediately to the other server.

Adding a User Map

To add a user map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose C, User Mapping.
3. Choose 8, Add a map.
4. In the Account field, type 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, type the name of the Unix user that you want to map to the NT user.
6. Choose 7, Save Changes.

Editing a User Map

To edit a user map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose C, User Mapping.
3. Select the letter of the map that you want to edit.
4. Choose 1, Edit Fields.

5. Enter your changes.
6. Choose 7, Save Changes.

Removing a User Map

To remove a user map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose C, User Mapping.
3. Select the letter of the user map that you want to delete.
4. Choose 8, Delete.

Adding a Group Map

To add a group map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose D, Group Mapping.
3. Choose 8, Add a map.
4. In the Account field, specify 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, specify the name of the Unix group that you want to map to the NT group.
6. Choose 7, Save Changes.

Editing a Group Map

To edit a group map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose D, Group Mapping.
3. Select the letter of the group map that you want to edit.
4. Choose 1, Edit Fields.

5. Enter your changes.
6. Choose 7, Save Changes.

Removing a Group Map

To remove a group map:

1. From the Extensions menu, choose CIFS/SMB Configuration.
2. Choose D, Group Mapping.
3. Select the letter of the group map that you want to delete.
4. Choose 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.

Objects residing on the system are classified according to the domain from which their 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, and are classified as Windows objects.

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.

The only time 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.

Objects can migrate from either domain to the other as the security attributes are changed. By default, however, only the migration from Unix to Windows is allowed. Specifically, a Unix object becomes a Windows object when its security attributes are changed using SMB.

The security attributes of a Windows object cannot be changed by reassigning its security attributes using NFS, because this could potentially weaken the access control protecting the object. Windows security is based on security descriptors, which cannot always be accurately represented using Unix security attributes. The NAS OS provides two mechanisms that allow the attributes of a Windows object to be modified using NFS, however: the `ch smb` command and the `acl.overwrite.allowed` environment variable. These are described separately below.

Using the `ch smb` Command

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, specify the absolute path to that object. `ch smb` does not perform recursive operations, so subdirectories or files contained within a directory are not 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 be careful 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.

Using the `acl.overwrite.allowed` Environment Variable

If the `acl.overwrite.allowed` environment variable is not defined or is defined as `NO`, the default volume behavior is applied; that is, the attributes of a Windows object cannot be changed using NFS.

If the `acl.overwrite.allowed` environment variable is set to `YES`, Unix commands, such as `chown`, `chgrp`, and `chmod` are permitted. 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.

Configuring the Host List

The console allows you to configure host information.

Note: In a cluster configuration, changes made to the host list on one server are propagated immediately to the other server.

Adding a Host

To add a host:

1. From the Configuration menu, choose Hosts.
2. Enter the new host name.
The system verifies that the host name does not already exist.
3. Press Enter to add the host.
4. Type the new host IP address.
5. Choose 7, Save changes.

Editing an Existing Host

To edit an existing host:

1. From the Configuration menu, choose Hosts.
2. Enter the name of the host you are editing.
3. Choose 1, Edit.
4. Type the new host name or IP address.
5. Choose 7, Save changes.

Deleting a Host

To delete a host:

1. From the Configuration menu, choose Hosts.

2. Enter the name of the host you are deleting.
3. Choose 8, Delete.

Managing Trusted Hosts

Use the Trusted Hosts menu option to manage hosts that have unrestricted access to all resources.

Note: In a cluster configuration, changes made to trusted hosts on one server are propagated immediately to the other server.

Adding a Trusted Host

To designate a trusted host:

1. From the Access Control menu, choose Trusted Hosts.
2. Enter a host name.

Note: To add a trusted host, the host must exist on the host list or NIS.

The system verifies that the trusted host name does not already exist. If the trusted host exists, the host information is displayed. If the host is not trusted, the system displays a warning.

3. Choose 7, Add to list.

The new trusted host is added, and the system displays the name at the top of the screen.

Deleting a Trusted Host

To delete a trusted host:

1. From the Access Control menu, choose Trusted Hosts.
2. Enter in the name of the trusted host to deleting.
3. Choose 8, Delete.

The trusted host is removed from the list.

4. If the removed trusted host loses access to any volumes currently mounted, unmount then remount those volumes. (exporting them first if necessary).

Managing Volume Access for NFS Clients

To manage volume access for NFS clients:

1. From the Access Control menu, choose Volume Access.
2. Type the letter corresponding to the volume for which you want 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.

Note: Do not allow any access, either read or write, to the `cvol` volume.

4. Choose 7, Save changes. Any existing NFS mounts are updated to reflect the new parameters.

Any changes to volume access affect the currently mounted volumes. For example, changing the access from read/write to none, will cause any currently mounted NFS clients to lose their connections.

In a cluster environment, access changes are made through the server that owns the volume. During and/or after a reboot of that server, the partner server will own the volume, and will recognize the changed access levels. When the volume fails over to the partner head, changes to the volume access can be made again, if required.

Locking and Unlocking the Console

You can disable or enable most of the main console menu options, preventing unauthorized use of those options. You must set the administrative password to secure the console.

In a cluster configuration, changes made to the lock/unlock status apply only to the server where you are logged in. Such changes do not propagate to the other server.

Locking the Console

To lock the console:

1. From the Operations menu, choose Lock Console.
2. Type the administrative password.
3. Select Y (Yes).

Unlocking the Console

To unlock the console:

1. From the main console menu, choose Unlock Console.
2. Type the administrative password.
3. Select Y (Yes).

Mirroring File Volumes

This section describes how to mirror file volumes from one NAS appliance (known as the active appliance) to another NAS appliance (the mirror appliance). It contains the following topics:

For more information on mirroring, see [Chapter 9](#).

- "[Configuring Active and Mirror Servers](#)" on page 272
- "[Configuring File Volumes](#)" on page 273
- "[Setting Warning Thresholds](#)" on page 275
- "[Breaking the Connection and Promoting a Mirrored File Volume](#)" on page 276
- "[Reestablishing a Mirror](#)" on page 278

Note: When using file replication with a cluster configuration, do not perform mirror operations (such as change role) when the cluster is in a degraded state.

Configuring Active and Mirror Servers

After the primary IP addresses have been configured on the active and mirror servers, and you have designated the roles of the ports connecting the two servers with one another as `Mirror`, configure mirroring on the active and mirror servers.

Configuring a New Active Server With a New Mirror Server

Follow these steps first on the active server and then, using Telnet, on the mirror server.

To configure a new active server with a new mirror server

1. From the Configuration menu, choose Host Names and Network.
2. Choose 1, Edit Fields.
3. If you have not done so already, configure the ports connected to a local network or subnet.

For more information about configuring TCP/IP using the console, see ["Configuring TCP/IP" on page 244](#). 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. Choose Save to save changes and return to the main console 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 250](#).

The network connections of the active and mirror systems are now configured. See the following section to continue.

Configuring an Existing Active Server With a New Mirror Server

To configure an existing active server with a new mirror server:

1. On the active server, from the Configuration menu, choose Host Names and Network.
2. Choose 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 reach the following command line:

```
connect to (? for list) ? [menu]
```
7. Log in as the administrator.
8. Type the following:

```
ping xxx.xxx.xx.xx
```

where `xxx.xxx.xx.xx` is the IP address of the mirror server.
9. On the mirror server, log in as administrator and type 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. You can only mirror file volumes equal to or larger than 1 gigabyte.

Note: After set up mirroring on a file volume, you cannot rename the file volume while maintaining the mirroring connection.

Setting Up a File Volume for Mirroring

Follow these steps to set up a file volume for mirroring, first on the active system and then on the mirror system:

1. Create a small (for example, 32-megabyte) file volume named SYS before creating any other volumes.
If you already have file volumes on the active system, this step is optional.
Do not create any other file volumes on the mirror system.
2. From the Configuration menu, choose 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. Type SYS for the name, and 64 for the size in megabytes (MB).
This forces residence of the /etc directory, and the configuration files it contains, on the SYS volume.

Mirroring File Volumes

To mirror file volumes:

1. Using Telnet, connect to the active system and access the main console menu.
2. From the Operations menu, choose Licenses.
3. Select the letter corresponding to Mirroring.
4. Type the activation key exactly as provided by Sun Microsystems.
5. Press Esc until you see the main console menu.
6. In the Extensions menu, choose Mirrors.
7. Choose Add mirror to create a new mirror.
8. Select the letter corresponding to the file volume to be mirrored.
The file volume must be equal to or larger than 1 gigabytes
9. Type the host name of the mirror system.
10. Type the private IP address, if necessary.
This is the IP address used for the mirroring connection with the mirror server.
11. Type the alternative IP addresses in the Alt IP Address fields.

12. If accessing the mirror server requires an administrative password, specify that password in the Remote admin password field.
 13. Enter the size of the Transaction Buffer Reserve.
 14. Choose 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. The volume is taken offline to avoid transient file system errors and inconsistencies.

During and after the mirror creation process, the system displays the Mirror Creation screen.
 15. To view the status of the mirror, choose A.
 16. To edit the alternate IP addresses or administrator password, choose 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. From the Extensions menu on the active server, choose Mirrors.
2. Choose 3, Threshold Config.
3. Choose 1, Edit to edit the percentages shown on this screen.
4. Type the desired percentages.
5. Type the number of hours the system must wait before reissuing the same threshold warning in the Alert Silent Period field.
6. Choose 7, Proceed.

Breaking the Connection and Promoting a Mirrored File Volume

To promote a file volume on the mirror server, you must first break the mirror connection. This section describes how to break the connection and promote a file volume. It contains these discussions:

- ["Breaking the Connection Between Mirror Servers" on page 276](#)
- ["Promoting a Mirrored File Volume" on page 277](#)
- ["Promoting iSCSI LUNs" on page 278](#)

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 down and you cannot access it to break the connection, you can break the mirror connection from the mirror server instead.

To break a mirror connection between mirror servers:

1. On the mirror system, view the status of the file volume by choosing Disks & Volumes from the Configuration menu.

The "*" (asterisk) appearing after the name of the mirrored file volume indicates that the file volume is currently mirrored.

Break the mirrored file volume from the mirror system only if the active system is down. To promote a file volume when the active system is up, break the mirror from the active system (not the mirror system).

2. From the Extensions menu, choose Mirrors.
3. Select the letter corresponding to the mirrored file volume that you are breaking.
4. Choose 8, Break.
Note: If possible, break the mirror from the active system.
5. When prompted to confirm the break, select Y (yes) to continue.
6. Press Esc to return to the main Mirrors screen.

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. After a mirror connection is broken and the mirrored file volume promoted, the original and mirrored file volumes are completely independent.

Note: There is no difference between promoting a compliance-enabled file volume and a non-compliance-enabled volume. The processing is identical.

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 276](#) for instructions. Then:

1. From the Extensions menu, choose Mirrors.
2. Choose 1, Promote Volume.
3. Select the letter corresponding to the file volume that you want to promote.
4. Choose 7, Proceed to promote the file volume (or 0 to cancel the request).
5. Indicate whether you want to assign a new name to the volume while promoting it: y (yes) or n (no).
If you respond with yes above, type the new name for the file volume on the next screen.
6. Confirm the promotion after reviewing your request. This processing cannot be reversed.
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.
7. When the system finishes promoting the file volume, press Esc to return to the main console menu.

If you want to configure NFS file volume access, continue with these steps:

8. Choose Volume Access from the Access Control menu.
9. Set the access rights to the file volume by selecting its corresponding letter.
10. Select Read/write, Read only, or None.
11. Choose 7, Save changes to continue.

The volume has now been promoted. From here:

- If the promoted file volume contains iSCSI logical unit numbers (LUNs), promote each iSCSI LUN next, as detailed under ["Promoting iSCSI LUNs" on page 278](#).

- To reestablish a mirror, see ["Reestablishing a Mirror"](#) on page 278.

Promoting iSCSI LUNs

After promoting a file volume that contains iSCSI logical unit numbers (LUNs), you must promote each iSCSI LUN on that file volume. To do this:

1. From the Extensions menu, choose iSCSI Configuration.
2. Choose A, Configure iSCSI LUN.
3. Choose 5, Promote a LUN.
4. Choose 1 to begin editing.
5. Enter the name of the file volume where the promoted iSCSI LUN resides (that is, the name of the file volume as it was just promoted).
6. Enter the iSCSI target IQN identifier for the LUN to be promoted.

The maximum size displays, along with a yes/no indication of whether the LUN is thin provisioned, and the alias (if available). The maximum size and thin-provisioned values are display-only and cannot be changed.
7. Enter (or modify) a brief description (alias) for the mirrored copy that you are promoting. For a cluster configuration, this might be filled in based on the original iSCSI LUN definition, but you can edit it.
8. Choose 7 to select the access list to be used with the promoted LUN. From the list that opens, either add a new access list for use with the LUN you are defining, or type the letter corresponding to the access list you want to use.
9. Choose 7 to save the current settings.
10. Press Esc to return to the main console menu.

Reestablishing a Mirror

This procedure describes how to reestablish a mirror when the active server has failed and you have promoted the file volume on the mirror server. The promoted file volume is now the most up-to-date version and functions completely independently of the out-of-date file volume on the active system. To recreate the mirror, mirror the up-to-date file volume back to the active server and then mirror the file volume back to the mirror server as it was originally.

If you have not promoted the mirrored file volume, do not follow these instructions. The active system 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.

Breaking the Mirror on Server 1

To break the mirror on Server 1:

1. On Server 1, in the Extensions menu, choose Mirrors.
2. Select the letter corresponding to the mirrored file volume.
3. Choose 8, Break.
4. Type Y (yes) to confirm breaking the mirror.

Deleting the Out-of-Date File Volume on Server 1

To delete the out-of-date file volume on Server 1:

1. Press Esc to return to the main console menu.
2. In the Configuration menu, choose Disks & Volumes.
3. Select the number corresponding to the mirrored file volume.

Caution: Before completing the following step, make sure you selected the out-of-date file volume on the active server (Server 1). Also make sure that the up-to-date file volume on the mirror server (Server 2) has been verified and promoted

4. Choose 8, Delete.
5. Type the file name of the out-of-date file volume.



6. Choose 7, Proceed with delete to delete the out-of-date file volume.

Mirroring the Up-to-Date File Volume on Server 2 Back to Server 1

To mirror the up-to-date file volume on Server 2 back to Server 1:

1. On Server 2, in the Extensions menu, choose Mirrors.
2. Choose 8, Add mirror.
3. Select the letter corresponding to the file volume that you are mirroring.
4. Type the private host name of Server 1.
5. Type the private IP address, if necessary, and the administrator password.
6. Type the transaction buffer reserve.

For more information, see ["To mirror file volumes:" on page 274](#).

7. Choose 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.

There can be no I/O activity to the mirror volume during synchronization. The volume is taken offline to avoid transient file system errors and inconsistencies while the mirror is being created.

You are now ready to change roles. See ["Changing Roles" on page 280](#).

Changing Roles

To change roles:

1. From the main console menu, select the Mirror option on Server 1.
2. Select the letter corresponding to the desired volume.
3. From the Mirror Status menu, select the Change Role option.
Note: Make sure the volumes are 100 percent in sync before changing roles.
4. Select Yes to confirm.

Monitoring

You can use the console to perform monitoring functions. The following sections describe how to set up and access monitoring functions:

- ["Configuring SNMP" on page 281](#)
- ["Configuring Email Notification" on page 281](#)
- ["Configuring Diagnostic Logs" on page 282](#)
- ["Viewing System Information" on page 284](#)

Configuring SNMP

The SNMP menu lets you send messages to a remote SNMP monitor, as well as modify the community string, contact information, and the location of the SNMP monitor.

To configure SNMP:

1. From the Extensions menu, choose SNMP Configuration.
Public is the default Community name. You can specify any name you want.
2. Make a selection as follows:
 - Choose 1-5, Edit a Trap Destination, to add, edit, or delete a trap destination.
 - Choose 6, Edit Community, to edit the community string.
 - Choose 7, Edit Contact, to edit contact information
 - Choose 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, the NAS appliance or gateway system 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, choose EMAIL Configuration.
2. Choose 1, Edit fields.
3. Type the information requested for each field. Press Enter to move between fields.
 - **SMTP Server** – This is the IP address or name of the server where all mail is directed. If you specify a name, it must be resolved by your DNS server. The host file or the DOS server must include the server name.
 - **Recipient 1-4** – These are the email addresses of the four people 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. Type 7, Save Changes to save the current configuration.
5. Press Esc to return to the main console menu.

Configuring Diagnostic Logs

The diagnostic log feature enables you to save or send diagnostic information in one file. The single compressed file, *diag.tar.gz*, contains all of the following information:

- *Diag.txt*, including information about the following:
 - Date and time
 - Uptime
 - CPU %
 - User
 - Software and OS
 - Hardware
 - Disk sub-systems
 - LUN paths
 - Disk error retry count
 - File systems
 - Network
 - Backup and Restore

- Windows share
 - ADS
 - CIFS
 - Mirroring
 - NTP
 - Environment
 - Enclosures
 - System Log
- Text entered in the Problem Description field
- Configuration and log files from /dvol/etc directory
 - passwd
 - group
 - hosts
 - approve
 - hostgrps
 - users.map
 - group.map
 - partner.log
- Local backup file under backup.directory
- Network capture file: netmdiag.cap.gz
- Files from /cvol/log
 - bootlog
 - dbglog
 - history
 - problem.txt
- RAID information from /dvol/support directory
- All syslog files

To create a diagnostic file at any time:

1. From the Extensions menu, choose Diagnostics.
2. Choose 2, Save File.
3. Choose 2, Save Diagnostics File.

The compressed file is stored in the default directory, /dvol/diagnostic, up to a maximum of two files.

To change the default directory:

1. Create the directory on a file volume with the exception of those with the FSOLF_READONLY attribute, /cvol, /proc, or a checkpoint.
2. From the Extensions menu, choose Diagnostics.
3. Choose 2, Save File.
4. Choose 1, Edit Path
5. In the PATH field, enter the complete path specification without the file name.

This location is now the default directory for all saved diagnostic files.

You can send the diagnostic file as an email message. See [“Sending a Diagnostic Email Message” on page 341](#).

Viewing System Information

You can view system information from the console.

Viewing Server Status

To view server status:

1. From the Operations menu, choose Activity Monitor.

The Activity Monitor screen lists the following information:

Field	Description
Volume	First 22 file volumes.
Use%	Amount of space used on the volume.
Reqs	Number of requests processed for the volume in the last 10 seconds.
Device	Name of the device.
Load	Percentage of CPU load.
Peak	Highest usage per second in the last 10 minutes.
Client	Name or address of the user.

2. Press Esc to return to the main console menu.

Viewing the System Log

To view the system log, choose Show Log from the Operations menu. The log displays two types of entries:

Type of Entry	Used to Report
System Startup Log Entries	Device configurations, volumes, and other pertinent information.
Normal Operation Log Entries	Device errors, security violations, and other routing status information. The version release number and software serial number are listed last.

Viewing Port Bonding

To view port bonding:

1. From the Configuration menu, choose Host Name & Network.
2. Press the spacebar to scroll to the next panel.

The bond1 column shows the first port bond. The input/output information in this column is the sum of the input/output information in the two ports that you bonded.

Viewing the Checkpoint Analysis

To view the checkpoint analysis:

1. From the Configuration menu, choose Disks & Volumes.
2. Type the letter corresponding to the drive that you are configuring.
3. Choose Change/Delete volume name.
4. Choose 6, Checkpoints.
5. Choose 3, Analysis. Scroll through the analysis using the spacebar.
6. Choose 0, End Analysis to exit this screen.

Viewing the Status of a Mirrored File Volume

To view the status of a mirrored file volume:

1. On the active system, choose Mirrors from the Extensions menu.
2. Select the mirrored file volume.

In 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:.

State	Description
ERR	An error has occurred.
NEW	A new mirror is being created.
INIT	The mirror buffer is being initialized.
MKPT	Disk partitions are being created on the mirror system.
RDY	The system is ready and waiting for the other system to be ready.
DOWN	The network link is down.
CRK	The mirror is cracked.
RPL	Replication 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, these fields have meaning as follows:

Field	Description
next xid	Next Transaction ID – ID of the next transaction for the file system.
sync xid	Sync Transaction ID – Last (synchronizing) transaction that was transferred to the mirror system.
head xid	Head Transaction ID – Last transaction that was acknowledged by the mirror system.

Field	Description
In Sync percentage indicator	When this field is at 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 performs a block-by-block resync. While the mirror state is in the Out Of Sync state, the mirror volume is volatile until the mirror is back in sync.

On the mirror system, these fields have meaning as follows:

Field	Description
next xid	Next Transaction ID – ID of the next transaction that is expected from the active system.
sync xid	Sync Transaction ID – Last transaction that was scheduled to be written to disk.
head xid	Head Transaction ID – Last transaction that was acknowledged on disk.
In Sync percentage indicator	When this field is at 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, choose 1, Edit.
4. Edit the fields, then choose 7, Proceed to save your changes.
5. To see network statistics on the mirrored file volume, choose 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, check to make sure that all network links are functioning properly. A fill rate greater than zero indicates transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. When the buffer overruns, the mirror is cracked.

Viewing Network Statistics for All Mirrored File Volumes

To view network statistics for all mirrored file volumes:

1. On the active system, choose Mirrors from the Extensions menu.
2. Choose 2, Network Statistics.

The screen displays the total number of RCBs (Request Control Blocks) sent, the number of RCBs sent per second, and the average size of the RCBs, as well as their average response time and transfer rate.

3. Choose 1, Reset to restart this display.

Configuring the NAS for iSCSI

Follow these steps to configure the NAS appliance or gateway system as an Internet Small Computer Systems Interface (iSCSI) target. This allows iSCSI initiators (host applications) to connect to, and access, iSCSI logical unit numbers (LUNs) on the NAS device:

1. Configure the iSCSI initiator client, referring to the documentation provided with the iSCSI initiator software.
2. Create one or more access lists, each comprising a list of iSCSI initiators that can access a specific set of iSCSI LUNs on the NAS device. Refer to "[Creating an iSCSI Access List](#)" on page 289 for further details. You will associate the appropriate access list with each LUN during LUN definition.
3. Configure one or more iSCSI LUNs, each corresponding to an area of storage on the NAS device that will be accessible to iSCSI clients. Refer to "[Creating an iSCSI LUN](#)" on page 290 for further details. Assign the appropriate access list to each LUN, to identify those iSCSI initiators that can access it.
4. If using the iSNS iSCSI target discovery method, configure an iSNS server, referring to "[Specifying an iSNS Server](#)" on page 291 for further details.

This section contains the following topics:

- "[Creating an iSCSI Access List](#)" on page 289
- "[Creating an iSCSI LUN](#)" on page 290
- "[Specifying an iSNS Server](#)" on page 291

Creating an iSCSI Access List

An Internet Small Computer Systems Interface (iSCSI) access list defines a set of iSCSI initiators that can access one or more iSCSI logical unit numbers (LUNs) on the NAS device.

Follow these steps to create or edit an iSCSI access list:

1. From the Extensions menu, choose iSCSI Configuration.
2. Choose B, Configure Access List.
3. Choose 7 to add a new access list (or type the letter corresponding to the list you want to edit).
4. Choose 1 to begin editing.
5. Enter the name of the access list, specified as any one or more characters.
6. Enter the full name of the Challenge Handshake Authentication Protocol (CHAP) initiator that is configured by the iSCSI initiator software (for example, `iqn.1991-05.com.microsoft:iscsi-winxp`).

If you leave this field blank, CHAP authorization will not be required. Refer to the iSCSI initiator documentation for more information.

7. Enter the CHAP password (minimum of 12 characters).
8. Enter the iSCSI Qualified Name (IQN) name of each client initiator that belongs to the list. Specify each name as any one or more characters. When you are though, press Enter with no initiator name specified.

CHAP ensures that the incoming data is sent from an authentic iSCSI initiator. If you do not specify at least one initiator IQN name, any initiator can access the target.

9. Choose 7 to save the current settings.
10. Press Esc to return to the main console menu.

Creating an iSCSI LUN

In order to configure the NAS appliance or gateway system as an Internet Small Computer Systems Interface (iSCSI) target, you must configure one or more iSCSI logical unit number (LUNs) that will be accessible to iSCSI clients. Each iSCSI LUN uses a dedicated storage area (on a standard NAS file volume) to provide physical storage for data processed by iSCSI client applications.

Before adding or editing an iSCSI LUN, ensure that you have created the corresponding access list for the LUN. For more information, see "[Creating an iSCSI Access List](#)" on page 289.



Caution: You can configure more than one iSCSI initiator to access the same target LUN; however, the applications running on the iSCSI client server must ensure synchronized access to avoid data corruption.

Follow these steps to create an iSCSI LUN:

1. From the Extensions menu, choose iSCSI Configuration.
2. Choose A, Configure iSCSI LUN.
3. Choose 7 to add a new iSCSI LUN (or type the letter corresponding to the iSCSI LUN you want to edit).
4. Choose 1 to begin editing.

5. Enter the name of the iSCSI LUN, specified as one or more alphanumeric characters (a–z, A–Z, 0–9), periods (.), hyphens (-), or colons (:).

The target name you specify will be prefixed with the full iSCSI Qualified Name (IQN) name according to the following naming convention:

`iqn.1986-03.com.sun:01:mac-address.timestamp.user-specified-name`

For example, if you type the name `lun1`, the full name of the iSCSI target LUN is:

`iqn.1986-03.com.sun:01:mac-address.timestamp.lun1`

Note: The timestamp is a hexadecimal number representing the number of seconds after 1/1/1970.

6. Enter a brief description (or alias) for the target LUN. Press Enter without typing a value to leave this field blank.
7. Enter the name of the NAS file volume where the iSCSI LUN will be created.
8. Enter the maximum size for the LUN, in bytes (*bytes* format), kilobytes (*bytesK* format), megabytes (*bytesM* format), or gigabytes (*bytesG* format). The minimum is capacity is 100 megabytes; the maximum capacity is 2 terabytes (2000G).

9. Select Y (yes) to create a thin provisioned LUN. A thin provisioned LUN sets the file size attribute to the specified capacity, but the disk blocks are not allocated until data is written to the disk.

If you create a non-thin provisioned LUN, disk blocks will be allocated based on the capacity of the LUN you are creating. When creating non-thin provisioned iSCSI LUNs, allow approximately 10% extra space on the volume for file-system metadata. For example, a 100 gigabyte iSCSI LUN must reside on a 110 gigabyte volume to allow non-thin provisioned LUN creation.

For more information about deciding to use thin provisioned or non-thin provisioned LUNs, see ["About SCSI Thin-Provisioned LUNs" on page 63](#).

10. Select 7 to select the access list to be used with this LUN. From the list that opens, either add a new access list for use with the LUN you are defining, or type the letter corresponding to the access list you want to use.
11. Choose 7 to save the current settings.
12. Press Esc to return to the main console menu.

Specifying an iSNS Server

An Internet Small Computer Systems Interface (iSCSI) initiator can locate its iSCSI NAS target using any of several methods, as detailed under ["About iSCSI Target Discovery Methods" on page 64](#). One such method is through an Internet Storage Name Service (iSNS) server, which enables iSCSI initiators to discover the existence, location, and configuration of iSCSI targets.

Follow these steps to enable use of an Internet Storage Name Service (iSNS) server for iSCSI target discovery. The NAS iSNS client inter-operates with any standard iSNS server, such as Microsoft iSNS Server 3.0.

To specify the iSNS server:

1. From the Extensions menu, choose iSCSI Configuration.
2. Choose C, Configure iSNS Server.
3. Choose 1 to edit the field shown.
4. Enter the Internet Protocol (IP) address of the iSNS server.
5. Choose 7 to save the current setting.
6. Press Esc to return to the main console menu.

System Maintenance

This section describes the system maintenance and setup functions that can be performed from the console, as follows:

- ["Configuring File Transfer Protocol \(FTP\) Access" on page 292](#)
- ["Shutting Down the System" on page 293](#)
- ["Managing Head Failover" on page 294](#)
- ["Configuring LUN Paths" on page 295](#)
- ["Scheduling File Checkpoints" on page 296](#)
- ["Configuring NDMP Backup" on page 296](#)
- ["Configuring System Auditing" on page 298](#)

Configuring File Transfer Protocol (FTP) Access

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

Types of Users

You can set up three types of users:

- **Administrators** who have the user name `admin` and use the same password used by GUI clients.
The administrator has root access to all volumes, directories, and files on the system. The administrator's home directory is defined as `/`.
- **Users** who have a user name and a password specified in the local password file or on a remote NIS or NIS+ name server.
The user has access to all existing directories and files within the user's home directory. The home directory is defined as part of the user's account information and is retrieved by the name service.
- **Guests** who log in with the user name `ftp` or its alias `anonymous`. A password is required but not authenticated. All guest users have access to all directories and files within the home directory of the `ftp` user.

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

Setting Up FTP Access

To set up FTP access:

1. From the Extensions menu, choose FTP Configuration.
2. Choose 1, Edit Fields.
3. Select Y (yes) to enable FTP or N (no) to disable it.

If FTP service is enabled, the FTP server will accept incoming connection requests.

4. In Allow guest access, select Yes to enable access to the FTP server by anonymous users or No to disable access.
5. In Allow user access, select Yes to enable access to the FTP server by all users or No to disable access.

This does not include the `admin` or `root` user.

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

6. In Allow admin access, select Yes to enable root access to those in possession of the Sun StorageTek administrative password (use with caution) or No to disable access.

Note: A root user has a user ID (UID) equal to 0, and the user name *admin*.

7. In Enable logging, select Yes to enable logging or No to disable logging.
8. If you enable logging, in Log filename specify the log file name.
9. Choose 7, Save changes.

Shutting Down the System

The NAS software is designed for continuous operation, but if you need to shut it down, you can do so from Web Administrator, the console, or the LCD panel.

To shut down the system:

1. From the Operations menu, choose 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 a previous software version. This option is available on systems that have more than one version of the software installed.
 - **ESC** – Press the Esc key to cancel and return to the main console menu.
- If you reboot, halt, or boot with a previous software version, the server reboots or turns off after all the delayed writes to disks are completed.

Managing Head Failover

In the event of a server failure, failover causes the working server to take temporary ownership of the Internet Protocol (IP) addresses and logical unit numbers (LUNs) formerly managed by the failed server. Follow the directions below enable server failover, and to initiate failback (recover).

Configuring Failover

To configure failover:

1. From the Extensions menu, choose Failover/Move LUNs.

Note: Failover/Move LUNs is available only in cluster configurations. You cannot enable or disable logical unit number (LUN) failover for a single-server system.
2. If the option is available, choose 3, Edit Failover.
3. Select Y (yes) to enable head failover.
4. Then:
 - Select Y (yes) to enable link failover. Link failover ensures that an alternate network link becomes active when a primary link fails.
 - Type the number of seconds before link failover occurs, in the event that one network link becomes unreliable.
 - Type the number of seconds before link restore occurs, in the event that the original link is repaired or reconnected.
5. Choose 2, Modify to rearrange logical unit number (LUN) ownership by adapter. When the restore process occurs, this is the resulting configuration.

- Type the LUNs owned by each adapter.
 - Separate the numbers by a single space (for example, 0 2 8 10).
 - Press Enter.
6. Select Y (yes) to save your changes.

Restoring the System, Initiating Failback

To restore the system, initiating failback:

1. Replace or repair the faulty component and make sure that it is online.
2. From the Extensions menu, choose Failover/Move LUNs.
Note: Failover/Move LUNs is available only in cluster configurations. You cannot enable or disable logical unit number (LUN) failover for a single-server system.
3. Choose 1, Restore.
4. Select Y (yes) to proceed with the restore process.

Configuring LUN Paths

See "[About Setting LUN Paths](#)" on page 17 for more information on logical unit number (LUN) paths subject and the use of the GUI in setting them.

To edit a LUN path:

1. From the Extensions menu, choose LUN Ownership.
The LUN Ownership screen displays all LUNs whose paths can be changed. A LUN can be reassigned only if there are no file systems on that LUN. For a cluster configuration, only the server that “owns” a LUN can reassign it to another server.
Note: With a cluster configuration, when you first start the system, all LUNs are assigned to one server (Head 1). You must use that server to reassign some LUNs to the partner server for even distribution.
Note: LUNs that have no LUN path assigned might initially appear multiple times in the LUN Ownership screen, as their presence is advertised by multiple controllers over multiple paths. After a LUN has a path assigned, it is shown once, on its current path.
2. Select a LUN path by typing the letter to the left of the desired path.

3. Choose 1, Edit to edit the LUN path.

The Configure LUN Path screen displays all the available paths for the LUN. The current or active LUN path is marked as `Active`. If the primary path is set for the LUN, it is marked as `Primary`.

4. Enter the number of the LUN path to which you want to change.

Evenly divide the assignment of LUNs to the two available paths. For example, the first and third LUN to path 1, and the second and fourth LUN to path 2.

5. Select Y (yes) to save your changes.

Scheduling File Checkpoints

A checkpoint is a virtual read-only copy of a primary file volume. See ["About File-System Checkpoints" on page 176](#) for detailed information about checkpoints.

To schedule checkpoints:

1. From the Configuration menu, choose 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. Choose 1, Edit.
4. Choose 6, Checkpoints.
5. Follow the prompts at the bottom of the screen, pressing Enter to tab through the fields.
6. After specifying all of the checkpoint information, choose 7, Save changes.

Configuring NDMP Backup

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 device.

By default, the current release uses V4 of NDMP, although V3 is supported. To verify the version, use the following command:


```
ndmp show version
```

To use V3, use the following command, but verify that no client systems use V4:

```
ndmp set version=3
```

To complete the configuration, you need to specify the complete paths to the devices. Use the following command to display the paths:

```
ndmp devices
```

To set up NDMP:

1. Configure the backup administration application to log in:
 - a. Enter the user name `admin`.
Note: In version 4.20, you specified the user name `administrator`.
 - b. Specify the same password used by the console administrator.
2. Configure the backup administration application to locate the devices on which the volumes reside. Specify the complete path to the device and the device's identifier, using the `ndmp devices` command.
Note: In version 4.20, you specified only the device's identifier.
3. For each file volume, verify that checkpoints are enabled and backup checkpoints are enabled. To view or set these settings, choose File Volume Operations > Edit Volume Properties
4. From the Extensions menu, choose NDMP Setup.
5. Select the network interface card (NIC) port adapter or bond port used to transfer data to the backup tape drive (typically an interface configured with independent role).
6. Press Enter.
7. Specify the full path, such as `/vol_ndmp`, for the directory used to store intermediate backup data and a permanent log of backup history. The directory must be independent from the volumes scheduled for backup, and at least 2 gigabytes in size.
8. Press Enter to save changes.

Configuring System Auditing

System auditing is a service that allows the administrator to audit particular system events by storing records of those events in log files. For more details about system auditing, refer to ["About System Auditing" on page 161](#).

To configure system auditing:

1. From the Extensions menu, choose System Audit Configuration.
2. Choose 1, Edit fields.
3. Enable auditing and specify the path for the audit log and the maximum file size for the log file.
4. Choose 7, Save changes to save changes.

Error Messages

This appendix describes the error messages produced by the various components of the NAS software. It includes the following sections:

- [“About Error Messages” on page 299](#)
- [“About SysMon Error Notification” on page 300](#)
- [“Reference: UPS Errors” on page 300](#)
- [“Reference: File-System Errors” on page 302](#)
- [“Reference: RAID Errors” on page 302](#)
- [“Reference: IPMI Events” on page 303](#)

About Error Messages

This appendix describes the specific error messages sent through email, Simple Network Management Protocol (SNMP) notification, the liquid crystal display (LCD) panel, and the system log to notify the administrator in the event of a system error. SysMon, the monitoring thread in the NAS software, monitors the status of redundant array of independent disks (RAID) devices, uninterruptible power supplies (UPSs), file systems, NAS servers, controller units, expansion units, and environmental variables. Monitoring and error messages vary depending on model and configuration.

About SysMon Error Notification

SysMon, the monitoring thread in NAS appliances and gateway systems, captures events generated as a result of system errors. It then takes the appropriate action of sending an email, notifying the Simple Network Management Protocol (SNMP) server, displaying the error on the liquid crystal display (LCD) panel, writing an error message to the system log, or some combination of these actions. Email notification and the system log include the time of the event.

Reference: UPS Errors

Refer to [TABLE B-1](#) for descriptions of uninterruptible power supply (UPS) error conditions.

TABLE B-1 UPS Error Messages

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Power Failure	AC Power Failure: AC power failure. System is running on UPS battery. Severity = Error Action: Restore system power.	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. Severity = Critical Action: Restore AC power as soon as possible.	EnvUpsLow Battery	U22 low battery	UPS: Low battery condition.
Normal Battery	UPS battery recharged: The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.

TABLE B-1 UPS Error Messages (Continued)

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Replace Battery	<p>Replace UPS Battery: The UPS battery is faulty. Severity = Notice Action: Replace the battery.</p>	EnvUps Replace Battery	U23 battery fault	UPS: Battery requires replacement.
UPS Alarms - Ambient temperature or humidity outside acceptable thresholds	<p>UPS abnormal temperature/humidity: Abnormal temperature/humidity detected in the system. Severity = Error Action: 1. Check UPS unit installation. 2. Contact Sun Services.</p>	EnvUps Abnormal	U24 abnormal ambient	UPS: Abnormal temperature and/or humidity detected.
Write-back cache is disabled.	<p>Controller Cache Disabled: Either AC power or UPS is not charged completely. Severity = Warning Action: 1. If AC power has failed, restore system power. 2. If after a long time the UPS is not charged completely, check the UPS unit and replace if necessary.</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. Severity = Critical Action: 1. Check the serial cable connecting the UPS unit to the NAS server, or 2. Check the UPS unit and replace if necessary.</p>	EnvUpsFail	U25 UPS failure	UPS: Communication failure.

Reference: File-System Errors

TABLE B-2 describes file-system error messages that occur when the file-system usage exceeds a defined usage threshold. The default usage threshold is 95 percent.

TABLE B-2 File-System Errors

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
File System Full	File system full: File system <name> is xx% full. Severity=Error) 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.	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is xx%.

Reference: RAID Errors

TABLE B-3 displays events and error messages for the redundant array of independent disks (RAID) subsystem.

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)

TABLE B-3 RAID Error Messages (*Continued*)

Event	Email Subject: Text	SNMP Trap	LCD Panel	Log
Controller Failure	RAID controller failure: RAID controller <i>N</i> has failed. Action: Contact Sun Services. Severity = Error	RaidControllerFa il	R12 Ctlr failure	RAID controller <i>N</i> failed.

Reference: IPMI Events

The NAS software uses the Intelligent Platform Management Interface (IPMI) board to monitor environmental systems, and to send messages regarding power supply and temperature anomalies. Device locations are shown in [Appendix D](#).

[TABLE B-4](#) describes the IPMI error messages for the NAS software.

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	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	envTemperatureError trap	P51 Temp error	The temperature is critical.
Primary Power Cord Failure	Power cord failure: The primary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envPrimaryPowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
Secondary Power Cord Failure	Power cord failure: The secondary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envSecondaryPowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

Compliance Archiving Software API

The NAS software supports strict compliance-archiving guidelines as a license-key-enabled software extension called “Sun StorageTek Compliance Archiving Software.

The Compliance Archiving Software is available in a stringent form (referred to as mandatory) and in a less stringent form (referred to as advisory). For overview information about the Compliance Archiving Software, see ["About Compliance Archiving Software" on page 147](#).

This appendix is a technical overview of the features and application programming interface (API) for the strict Compliance Archiving Software. It contains the following sections:

- ["Compliance Features" on page 306](#)
- ["Accessing Compliance Functionality" on page 308](#)
- ["Unix System Calls with Compliance Archiving" on page 312](#)
- ["Behavior of Windows Clients" on page 315](#)
- ["Other APIs" on page 317](#)

For Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems, proper operation of the Compliance Archiving Software requires the correct physical configuration of the NAS appliance or gateway-system hardware. In particular, the redundant array of independent disks (RAID) controller must not be connected to any device or network, other than a private Fibre Channel connection to the NAS server, and (for non-gateway configurations), connections to any expansion units. There are no such requirements for Sun StorageTek 5210 NAS appliances.

To ensure the strongest possible enforcement of your data retention policies, you must also provide for the physical security of your NAS device. 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 operates on file volumes that have been created as compliance-enabled. Its functionality consists of these major features:

- ["WORM Files" on page 306](#)
- ["File Retention Periods" on page 307](#)
- ["Administrative Lock-Down" on page 307](#)
- ["Compliance Audit" on page 308](#)

For test environments or for deployments with less stringent requirements, the Compliance Archiving Software provides the option of advisory enforcement that overrides some of these features.

With the standard mandatory enforcement, no one can delete a WORM file before its retention date, decrease a WORM file's retention time, or delete a compliance volume. Under the advisory enforcement option, authorized administrator can decrease a WORM file's retention time and delete a WORM file before its retention date. These operations are logged in the audit log.

Note – File volumes that are compliance-enabled might have slightly lower performance than volumes without this protection.

WORM Files

The term "WORM" means "write-once, read-many" and indicates that the file is archived in non-rewritable, non-erasable storage. A more accurate description is to call these files "permanent read-only" files.

A file can be created with the normal access controls and modified as needed, but after it becomes a WORM file, the Compliance Archiving software enforces stronger access controls than the traditional file access semantics provided by the NFS and CIFS protocols.

When a data management application designates a file as WORM, the file becomes permanently immutable. WORM files cannot be modified, extended, or renamed. A WORM file can be deleted only when its retention time has been met and in accordance with the file retention rules.

In addition to providing storage for WORM files, the Compliance Archiving System supports backup to immutable tape media, or WORM tape.

Note – Checkpoint files cannot be restored over write-once, read-many (WORM) files.

File Retention Periods

The Compliance Archiving Software associates a retention period with each WORM file. If you or the data management application that writes files to the volume does not set a retention period explicitly for each file, the default retention period is used.

When the retention period expires, you can delete a WORM file or extend its retention period. With the advisory compliance option, you can decrease the retention period for a file to allow it to be deleted. With the mandatory compliance option, you cannot decrease the retention period.



Caution – If you or the data management application that writes files to the volume does not set a retention period explicitly for each file before making the file WORM, the default retention period for the volume is used. You can change the volume's default, but under mandatory compliance, this default retention period is permanent.

Administrative Lock-Down

Some system administration functions are disabled or restricted on compliance-enabled file volumes to ensure the retention and preservation assurances of WORM files and retention periods. These restrictions affect functions that could be used to circumvent a file's retention, for example, by deleting the file's volume.

Compliance Audit

The Compliance Archiving Software retains immutable records of all compliance-related activities that occur on the system. It maintains a text-based log file for attempted efforts to modify or delete data, with or without proper authority, and is enabled through the use of the Data Retention Audit Service (DRAS) API, which includes the following features:

- Accountability of changes and attempted changes to retained files
- A logging mechanism through which events that are audited are stored
- Protection and preservation of the audit log for the life of the system
- The log is in a viewable format and has secure access through standard system access protocols.

The following events are audited:

- 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

A full description of the audit log provided by this service is in [Chapter 9](#).

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 NAS appliance or gateway system (NFS and CIFS). In particular, the NAS device 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 NAS appliance or gateway system, where only some of which are compliance-enabled.

Do 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. After 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 must be converted to a WORM file.

The WORM trigger for Unix clients is setting a file's permission mode to 4000. Client applications or users can invoke this WORM trigger using the `chmod` command or system call. On receiving this request, the Compliance Archiving Software converts the target file into a WORM file by doing the following:

- Setting the setuid bit
- Clearing any write bits that are set on the file
- Retaining any read access bits on the file

Note: Executable files cannot be made into WORM files. For files created from Windows clients, this means that a file cannot be made into a WORM file if its access control list (ACL) has any access control entries (ACEs) granting execute permission on the file.

In the following example, a file with an access mode of 640 is converted to a WORM file. After the WORM trigger is issued, the file's access mode is 4440.

```
$ ls -l testfile
-rw-r----- 1 smith  staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr----- 1 smith  staff      12139 Dec  2 13:18 testfile
```

The Compliance Archiving Software uses this WORM trigger because it is an operation that is unlikely to be used by existing applications.

The WORM trigger for Windows clients is setting both the read-only and the system bit on a file. Setting these bits will only trigger WORM if neither the archive nor hidden bits are set on the file. The WORM trigger sets the file's read-only bit, but does not change its system bit. Use the following command to enable the WORM trigger:

```
hostname> fsctl compliance wte on
```

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 setuid bit• Modify size or modification time (mtime)
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 (mtime)

WORM Restrictions

The Compliance Archiving Software does not allow WORM files to be renamed. Furthermore, non-empty directories cannot be renamed. This rule guarantees that the full pathname of a WORM file cannot change for the lifetime of the file.

When a Unix client sets a file mode to 4000 (invoking the WORM trigger), the resulting access mode on the file will 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. Any attempt to remove a WORM file prior to the end of its retention period will fail.

Compliance Archiving retention timestamps are stored in the access time (`atime`) attribute of WORM files.

Note: 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 operations, regardless of whether a file is a WORM file.

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.

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 client user or application does not specify a retention period, or the `atime` attribute represents a time in the past, the Compliance Archiving Software uses the default retention period specified for the volume when it was created.

To specify that a permanent retention, set the file's `atime` to the maximum legal value for a signed 32-bit integer (`0x7fffffff`). On Unix systems, this value is defined as `INT_MAX` in the `limits.h` header file. and translates to a timestamp of 03:14:07 GMT, Jan 19, 2038.

You can extend retention periods, and set new retention periods for files whose retentions are expired, as long as the new value represents a time later than the old retention timestamp. To extend the retention, reset the `atime` attribute on the WORM file.

Client applications and users can determine the retention status of a file by reading the file's attributes, using standards tools and APIs. Unix clients, for example, can read a file's attributes using the `stat(2)` system call. Unix users can view a file's attributes using the `ls-lu` command, which lists files with their access permissions and `atime` timestamps.

Unix System Calls with Compliance Archiving

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 NAS share. System calls not listed here behave as normal.

It is important to remember that the interfaces to the NAS appliance or gateway system are the NFS and CIFS file access protocols. Thus, this section incorporates both the compliance-related behavior of the NAS device 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 clients and must 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 315](#).)

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 NAS appliance or gateway system 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

This section describes the differences in compliance-enabled files for Windows clients.

Creating WORM Files

A regular, non-WORM file can be converted to a WORM file from Windows only if its archive and hidden bits are not set. If these bits are cleared, a Windows client converts the file to a WORM file by setting its read-only and system bits. This WORM trigger will result in setting the file's read-only bit, but will not change the state of the file's system bit.

Metadata Restrictions on WORM Files

Windows clients can change the archive bit on a WORM file but they cannot 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.

WORM File's 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 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 might become WORM files because their read-only and system bits set.

Compliance and Antivirus Software

When you enable antivirus protection on a compliance-enabled volume, the following cases are handled in a special manner:

- If a file is scanned for viruses before it is retained and found to be infected, the file is quarantined. Quarantined files are not retained.
- If a retained file is scanned for viruses and found to be infected, access is denied.

For more information about virus scanning, see [Chapter 4](#).

Many virus-checking programs attempt to preserve the access time on the files they examine. These programs read a file's `atime` before checking it for viruses, and afterwards, reset the `atime` to the value it had before the scan. This can lead to a race condition if the virus-checking program scans a file at the same time that another application is setting a retention time on the file. As a result, the file might have the wrong retention time.

To avoid this problem, make sure that virus-checking software does 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.

Appliance and Gateway System Components

This appendix describes the hardware components for the Sun StorageTek 5320 NAS server, the Sun StorageTek 5220 NAS appliance, and for the RAID components used with Sun StorageTek 5310, Sun StorageTek 5220, and Sun StorageTek 5320 NAS appliances and gateway systems. For related information:

- Refer to the *Sun StorEdge 5210 NAS Hardware Installation, Configuration, and User Guide* for information about Sun StorageTek 5210 NAS appliance hardware components.
- Refer to the *Sun StorEdge 5310 NAS Appliance and Gateway System Getting Started Guide* for details about the Sun StorageTek 5310 NAS server components.
- For gateway systems, refer to your NAS appliance and gateway system *Getting Started Guide* for information about connecting to SAN storage (a Sun StorageTek 6130 array, Sun StorageTek Flexline 280 and 380 storage systems, Sun StorageTek 6920 system, and so forth).

This appendix includes the following topics:

- [“The Sun StorageTek 5320 NAS Server” on page 320](#)
- [“Sun StorageTek 5320 Controller Units and Expansion Units” on page 328](#)
- [“Sun StorageTek 5220 NAS Appliance” on page 338](#)

See [Chapter 12](#) for information about components that are identified as customer-replaceable units (CRUs).

The Sun StorageTek 5320 NAS Server

The Sun StorageTek 5320 NAS server is the basic server unit for all appliance and gateway-system configurations. [FIGURE D-1](#) shows the front of the server.

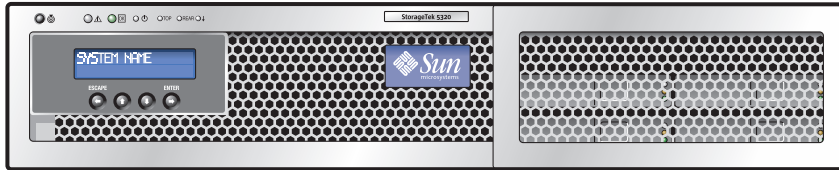


FIGURE D-1 Sun StorageTek 5320 NAS Server Front View

In cluster configurations, there are two high-availability (HA) servers, identified in their software serial numbers as server H1 and server H2.

This section describes the server, as follows:

- [“Front Panel Buttons and LEDs” on page 321](#) describes the buttons, LEDs, and Liquid Crystal Display (LCD) panel on the front of the server.
- [“Back Panel Ports and LEDs” on page 323](#) describes the LEDs on the back of the server, and provides instructions to connect the server to a local UPS (uninterruptible power supply) device.

Front Panel Buttons and LEDs

The front of the server provides a power button, LEDs, and Liquid Crystal Display (LCD) panel, illustrated in [Figure D-2](#), then described in detail.

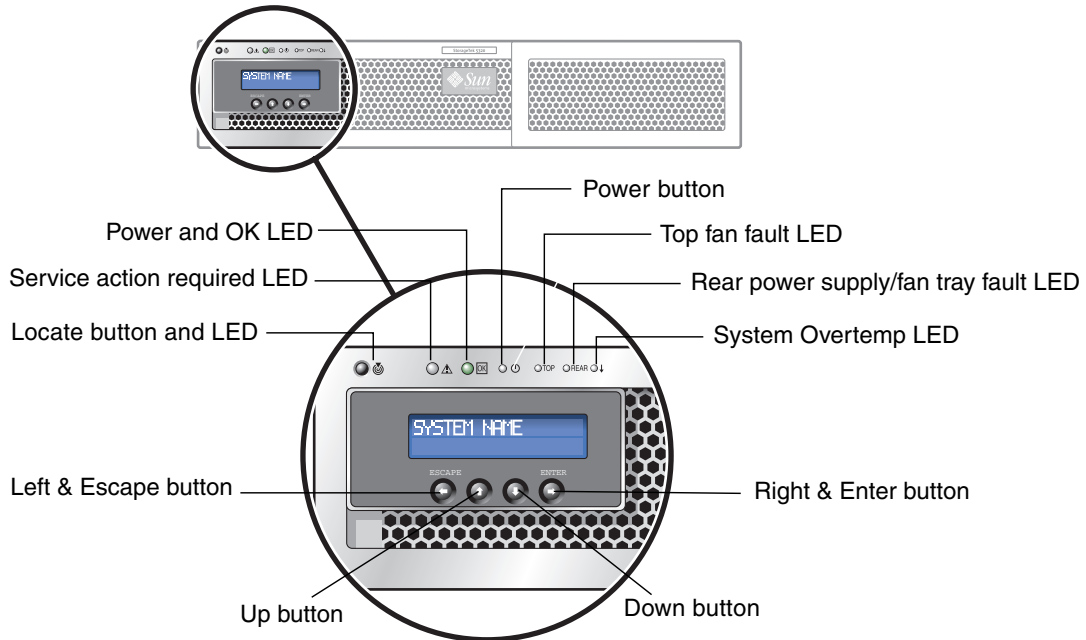



FIGURE D-2 NAS Server Front Panel Buttons and LEDs

Power Button

The power button () turns power on to the NAS server. Use a pen tip or similar implement to press and release the recessed button.



Caution: Do not use the power button to shut down the system. Always use the LCD menu or remote shutdown procedure described in [“Shutting Down the Server” on page 174](#). Improper shutdown can result in a loss of data.







Always power on the system components in this sequence:

1. Array expansion units
2. Array controller units

3. NAS server

Status Indicator LEDs

The LEDs on the front of the NAS server provide a status of server components, and help in locating the server in a rack, as described below:

LED	Description
Locate button/LED 	This LED helps you to identify which system you are working on, in a rack that contains multiple servers. <ul style="list-style-type: none">• Push and release this button to make the Locate LED blink for 30 minutes.• Hold down the button for 5 seconds to initiate a "push-to-test" mode that illuminates all other LEDs both inside and outside of the chassis for 15 seconds.
Service action required LED 	This LED has two states: <ul style="list-style-type: none">• Off: Normal operation.• Slow blinking: An event has been detected that requires a service action.
Power/OK LED 	This LED has three states: <ul style="list-style-type: none">• Off: Server main power and standby power are off.• Blinking: Server is in standby power mode, with AC power supplied only to the GRASP board and the power supply fans.• On: Server is in main power mode with AC power supplied to all components.
Top fan fault LED 	This LED lights when there is a failed front cooling fan module. LEDs on the individual fan modules indicate which fan module has failed.
Rear power supply/fan tray fault LED 	This LED lights when: <ul style="list-style-type: none">• Two power supplies are present in the server, but only one has AC power connected. To clear this condition, either plug in the second power supply or remove it from the chassis.• A voltage-related event occurs in the system. For CPU-related voltage errors, the associated CPU Fault LED will also be illuminated on the motherboard.• The rear fan tray has failed or is removed.
System overtemp LED 	<ul style="list-style-type: none">• This LED lights when an upper temperature limit is detected.

LCD Menu and Buttons

The LCD displays the server name and CPU utilization, and provides a menu that lets you perform basic local functions, including changing network configuration settings, and shutting down or rebooting the system.

When you shut down the system using the LCD buttons, the server performs a graceful shutdown under operating system control. Remote users can shut down the system through the network using the Web Administrator graphical user interface.

The following buttons (located below the LCD) are used to navigate through the LCD menu options.

LCD Button	Description
Left/Escape button	Undo, Backspace, Escape.
Up button	Scrolls up and selects characters, dots, spaces.
Down button	Scrolls down and selects characters, dots, spaces.
Right/Enter button	Accept, Select, Save, Enter.

Back Panel Ports and LEDs

The back of the server contains a dual-port Fibre Channel (FC) host bus adapter (HBA) card in PCI slot 1, can optionally contain a second dual-port FC HBA card in PCI slot 0, for high availability. [FIGURE D-3](#) shows the back of the server.

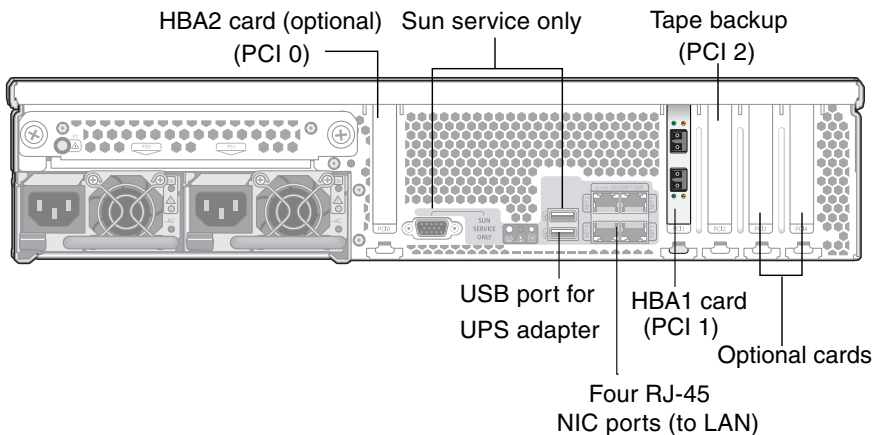


FIGURE D-3 NAS Server Back Panel With Single HBA Card

Each server contains can contain other optional cards, as detailed in the *Getting Started Guide* for your appliance or gateway system.

The topics below provide detail for:

- “[Back Panel LEDs](#)” on page 324 describes the LED indicators on the back of the server.
- “[Server Power Supplies](#)” on page 325 describes the two redundant hot-swappable power supplies.
- “[Direct-Attached Tape Library](#)” on page 326 describes the optional use of PCI 2 to attach to a tape library.

Back Panel LEDs

The LEDs on the back of the server are illustrated in [FIGURE D-4](#), then described following that figure.

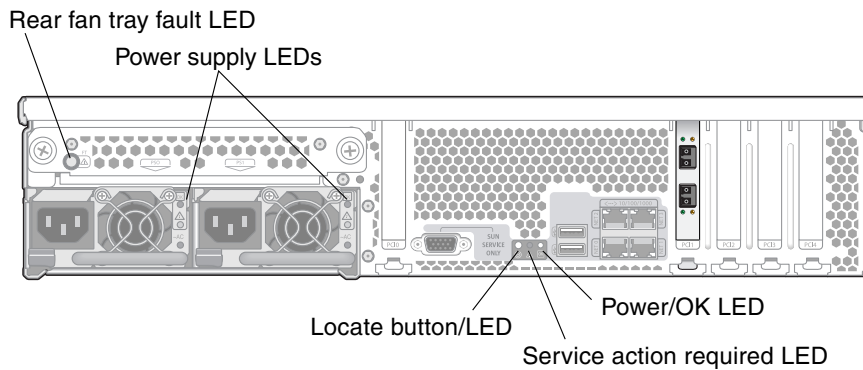


FIGURE D-4 Server Back Panel LEDs

The LEDs on the back of the NAS server provide a status of server components, and help in locating the server in a rack. The LEDs are described below, left-to-right as you face the back of the server.

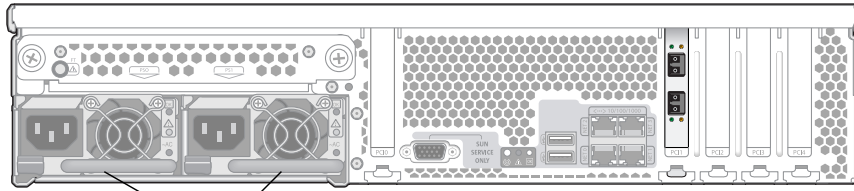
LED	Description
Rear fan tray fault LED	This LED has two states: <ul style="list-style-type: none">• Off: Fan module is OK.• Lit (amber): Fan tray has failed.

LED	Description
Power supply LEDs	The power supplies each have three LEDs: <ul style="list-style-type: none"> • Top LED (green): Power supply is OK. • Middle LED (amber): Power supply failed. • Bottom LED (green): AC power to power supply is OK.
Locate button/LED	This LED helps you to identify which system you are working on, in a rack that contains multiple servers. <ul style="list-style-type: none"> • Push and release this button to make the Locate LED blink for 30 minutes. • Hold down the button for 5 seconds to initiate a "push-to-test" mode that illuminates all other LEDs both inside and outside of the chassis for 15 seconds.
Service action required LED	This LED has two states: <ul style="list-style-type: none"> • Off: Normal operation. • Slow blinking: An event has been detected that requires a service action.
Power/OK LED	This LED has three states: <ul style="list-style-type: none"> • Off: Server main power and standby power are off. • Blinking: Server is in standby power mode, with AC power supplied only to the GRASP board and the power supply fans. • On: Server is in main power mode with AC power supplied to all components.

Server Power Supplies

A system's power supply provides power to all of its components. The power supply systems for all units are auto-sensing devices, with automatic adoption to line voltages from 100 to 240 volts, 50 to 60 Hz.

The power supply system in the server comprises two redundant hot-swappable modules in a 1 + 1 configuration, as shown in [FIGURE D-5](#). Each module is capable of maintaining a load of 500 watts. One power supply is required for system operation, with the second power supply providing power redundancy.



Power supply modules

FIGURE D-5 Power Supply Modules

Each power supply has the following capabilities:

- 550 watt output
- Internal multi-speed cooling fans
- Built-in load sharing
- Built-in overload protection
- Integral handle for ease when inserting/extracting the device

In a cluster configuration, if one of the servers experiences a power failure, both servers are rebooted under OS control. In this configuration, both servers detect the failure and reset themselves to correct the failure.

Direct-Attached Tape Library

You can attach a local tape backup device through the SCSI port on the back of the server (PCI slot 2). Set the SCSI ID of the tape library to be lower than the tape drive ID. For example, you might set the library ID to 0 and the drive ID to 5.

Make sure the tape device you attach is supported by the NAS appliance or gateway system. For the most current information on supported tape devices, contact your Sun sales representative.

TABLE D-1 Sun StorageTek 5300 RAID-5 Possible Configurations

Controller Enclosure (FC only) or Expansion Enclosure	Total Drives	Raw Capacity	Stripe	RAID-5 Sets	Hot Spare	Usable LUN Capacity
146 GB FC drives	14	2.044 TB	1	5+1, 6+1	1	1.46 TB

TABLE D-1 Sun StorageTek 5300 RAID-5 Possible Configurations (*Continued*)

Controller Enclosure (FC only) or Expansion Enclosure	Total Drives	Raw Capacity	Stripe	RAID-5 Sets	Hot Spare	Usable LUN Capacity
	7	1.022 TB	1	5+1	1	0.73 TB
300GB FC drives	14	4.2 TB	1	5+1, 6+1	1	3.3 TB
	7	2.1 TB	1	5+1	1	1.5 TB
400 GB SATA drives	14	5.6 TB	1, 2	5+1, 6+1*	1	4.0 TB
	7	2.8 TB	1	5+1	1	1.82 TB

* These RAID Set drives are striped into two volumes.

If a power supply fails, the Rear LED will light on the server. Contact Sun Services to replace the failed power supply.

Sun StorageTek 5320 Controller Units and Expansion Units

This section describes the hardware components for Sun StorageTek 5320 controller units and expansion units, as follows:

- [“Controller Units” on page 328](#) provides an overview of the 5320 controller units, including RAID capacity.
- [“Expansion Units” on page 332](#) provides an overview of the 5320 expansion units, including RAID capacity, indicators and LEDs, and the battery backup compartment.
- [“Mixed FC and SATA Capacity” on page 335](#) provides guidelines to follow when combining Fibre Channel (FC) and Serial Advanced Technology Attachment (SATA) drives.
- [“Disk Drives” on page 336](#) provides an overview of the 5320 drive shuttles, including information about failures and how to locate a particular physical drive.

Controller Units

Sun StorageTek 5320 controller units provide back-end storage for appliance (non-gateway) configurations. For increased capacity, they can be used with Sun StorageTek 5320 Expansion Units (see [page 332](#)).

Each controller unit and expansion unit contains either 8 or 16 redundant array of independent disks (RAID) drives of a single drive type (either Fibre Channel (FC), or Serial Advanced Technology Attachment (SATA)).

- The FC controller unit contains either 8 or 16 hot-swappable hard drives organized as one or two redundant array of independent disks (RAID)-5 sets, respectively, plus one global hot-spare. The RAID sets are pre-configured: the first 8 drives as one hot spare plus one 6+1 RAID set; the remaining half, if used, as a 7+1 RAID set.

For FC drives, the 6+1 RAID set forms a single volume, and the 7+1 RAID set, if present, forms two volumes of equal size.

- The SATA controller unit also contains either 8 or 16 hot-swappable hard drives, organized into RAID sets as described above for the FC drives. Each SATA RAID set forms two volumes of equal size.

The table below summarizes the possible configurations for each type of supported drive. Check the release notes for any additional supported drives.

TABLE D-2 Sun StorageTek 5320 RAID-5 Possible Configurations

Drive type	Total Drives	Raw Capacity	RAID-5 Sets	Hot Spare	Usable LUN Capacity
300 GB FC drives (2GB FC 10K RPM)	16	4.8 TB	6+1, 7+1*	1	3.8 TB
	8	2.4 TB	6+1	1	1.7 TB
500 GB SATA drives (SATA II 7.2K RPM)	16	8.0 TB	6+1*, 7+1*	1	6.0 TB
	8	4.0 TB	6+1*	1	2.8 TB

* These RAID Set drives are striped into two volumes.

In addition to the hard drives, the controller unit houses two RAID controllers and two power supplies.









Front of the Controller Unit



The following list describes the components on the front of the controller unit.

Ports/Switches	Description
Ports (Ch 1 and Ch2)	Two 2-Gbit/second FC Small Form-factor Plug-in (SFP) ports.
Expansion ports (P1 and P2)	Two 2-Gbit FC ports used to connect to the drive channel device and expansion units.
Power supplies	Two power supplies with battery backup. The power supplies provide redundant power to both controllers. If one power supply fails, both controllers are powered by the other power supply.
Battery backup compartments	Battery backup to maintain the integrity of the controller's data cache for up to 72 hours in the event of power loss to both power supplies. See "Battery Backup Compartments" on page 331 for more information.

Back of the Controller Unit

The following table describes the LEDs and components on the back of the controller unit. Keep in mind that a particular tray LED icon might not be visible unless the LED is illuminated.

LED/Indicator	Description
<i>Power Supply LEDs</i>	
DC 	On indicates that the correct DC power is being output from the controller power supply.
Service Action Required 	Steady amber indicates that the power supply requires service. Off indicates that the power supply does not require service.
Service Action Allowed 	Steady blue indicates that service action can be taken on the power supply without adverse consequences. Off indicates that the power supply is engaged and service action must not be implemented.
AC 	On indicates that AC power is being supplied to the controller power supply.
<i>Controller LEDs</i>	
ID/Diag display	Seven-segment readouts indicate the ID of the tray.
Cache Active 	Steady green indicates that data is in the cache. Off indicates that all data has been written to disk and the cache is empty.
Service Action Required 	Steady amber indicates that the controller requires service. Off indicates that the controller does not require service.
Service Action Allowed 	Steady blue indicates that service action can be taken on the controller without adverse consequences. Off indicates that the controller is engaged and service action must not be implemented.
<i>Controller Indicators</i>	
Host Port Rate 	The combined display indicates the host port link rate for the tray: LED 1 Off, LED 2 On – 2 Gbits/second

LED/Indicator	Description
Expansion Port Rate 	The combined display indicates the expansion port link rate for the tray: LED 4 Off, LED 2 On – 2 Gbits/second
Expansion Port Bypass 	Steady amber indicates that no valid device is detected and that the drive port is bypassed. Off indicates that there is no small form factor plug-in (SFP) transceiver installed or that the port is enabled.
Ethernet Status (on upper left-side of Ethernet connector)	Steady green indicates that there is an active connection. Off indicates that there is not an active connection.
Ethernet Rate (on upper right-side of Ethernet connector)	Steady green indicates that there is a 100BaseTX connection to the port. Off (when Ethernet Status LED is on) indicates that there is a 10BaseT connection to the Ethernet port.

Battery Backup Compartments

The controller unit has one battery backup compartment for each controller, which houses a battery used for power backup. [FIGURE D-6](#) shows the location of the battery compartments on the controller unit, and identifies the LEDs on the compartment.

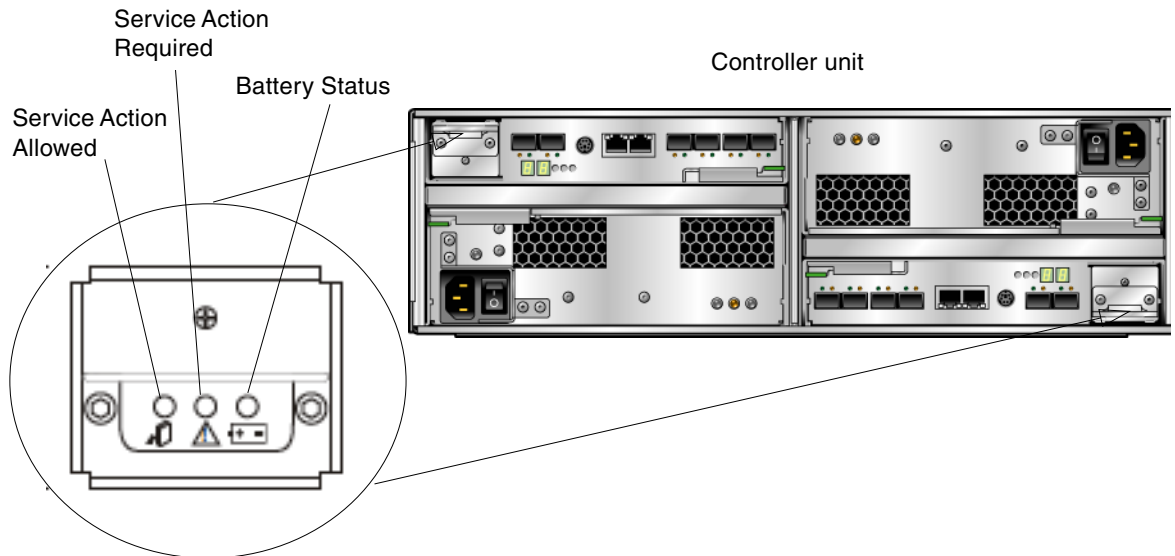





FIGURE D-6 Sun StorageTek 5320 Controller Unit Battery Backup Compartment LEDs

TABLE D-3 describes the LEDs on each battery backup compartment.

TABLE D-3 Battery Backup Compartment LEDs

LED/Indicator	Description
Service Action Allowed 	Steady blue indicates that service action can be taken on the power supply without adverse consequences. Off indicates that the power supply is engaged and service must not be implemented.
Service Action Required 	Steady amber indicates that the power supply requires service. Off indicates that the battery does not require service.
Battery Status 	Steady green indicates that the battery is fully charged. A slow blink indicates that the battery is charging. Off indicates that the battery is discharged or off.

Expansion Units

Sun StorageTek 5320 expansion units allow you to extend the storage capabilities of an array that is configured behind a Sun StorageTek 5320 controller unit.

Each expansion unit is configured for either Fibre Channel (FC) or Serial Advanced Technology Attachment (SATA) storage, exactly in the same way as described for the controller units starting on [page 328](#).

Ports and Power Supplies

FIGURE D-7 shows the ports and power supply on the back of the expansion unit.

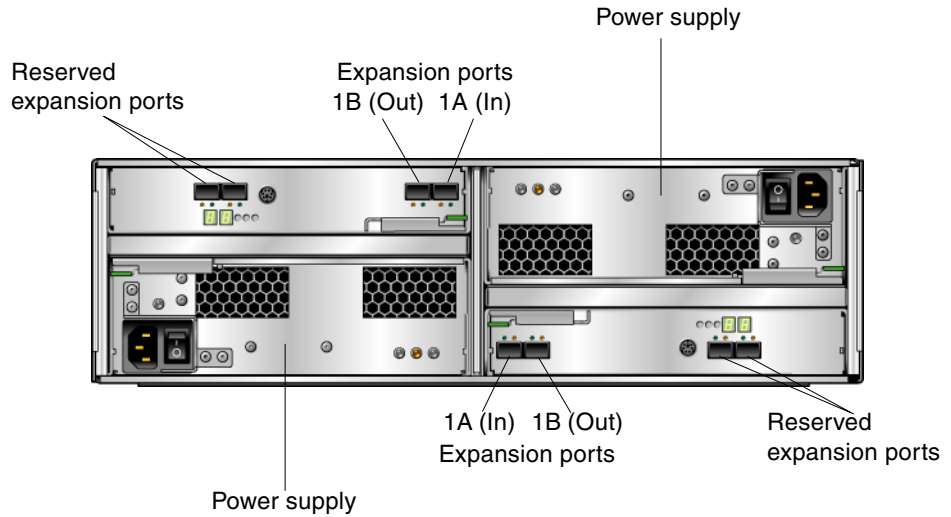


FIGURE D-7 Sun StorageTek 5320 Expansion Unit Ports and Components

The table below describes these ports and components:

Ports/Switches/LEDs	Description
Expansion ports 1A (In), 1B (Out)	Two 2-Gbit FC ports used to connect to an array controller and/or additional expansion units.
Power supplies	For each expansion unit, two power supplies that provide redundant power to the tray. If one power supply fails, the tray is powered by the remaining power supply.
Reserved expansion ports	Reserved for future use.

LEDs and Indicators

FIGURE D-8 shows the LEDs and indicators on the back of the expansion unit.

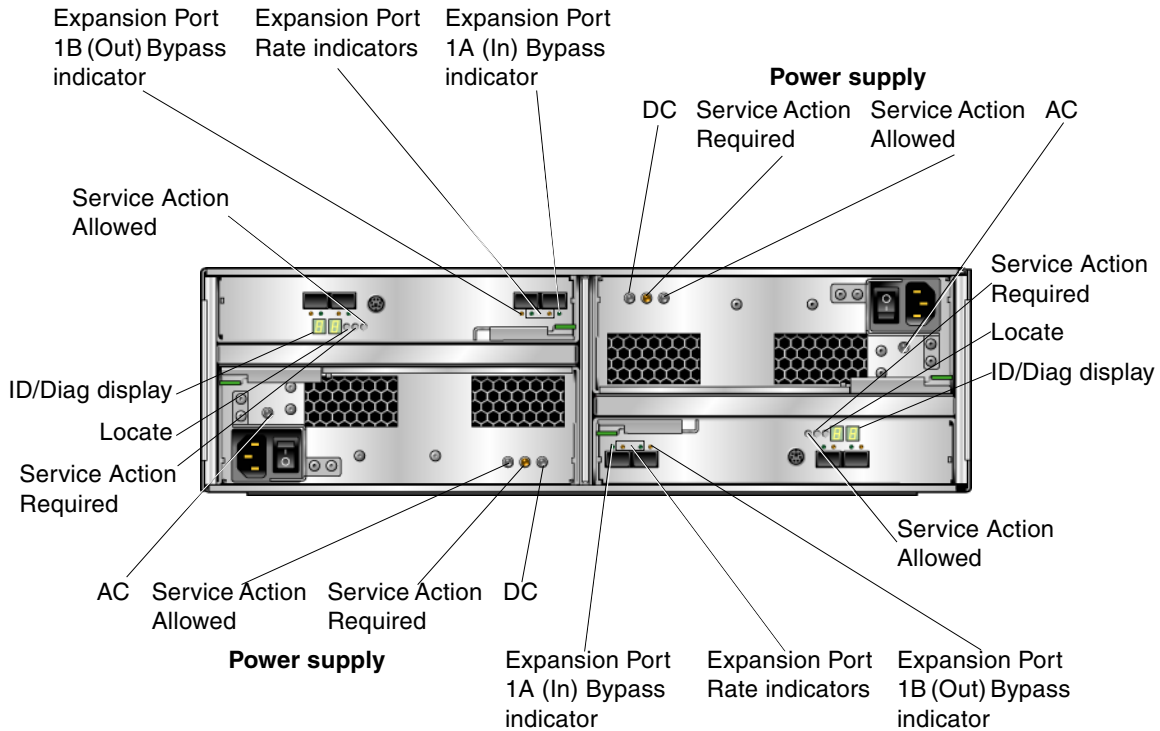











FIGURE D-8 Sun StorageTek 5320 Expansion Unit LEDs and Indicators

The following table describes the LEDs and indicators at the back of the expansion unit.

LED/Indicator	Description
<i>Power Supply LEDs</i>	
DC 	On indicates that the correct DC power is being output from the controller power supply.
Service Action Required 	Steady amber indicates that the power supply requires service. Off indicates that the power supply does not require service.

LED/Indicator	Description
Service Action Allowed 	Steady blue indicates that service action can be taken on the power supply without adverse consequences. Off indicates that the power supply is engaged and service action must not be implemented.
AC 	On indicates that AC power is being supplied to the controller power supply.
<i>Expansion Unit LEDs</i>	
ID/Diag display	Seven-segment readouts indicate the ID of the tray.
Locate 	Steady white identifies the controller after initiation from the management station.
Service Action Required 	Steady amber indicates that the controller requires service. Off indicates that the controller does not require service.
Service Action Allowed 	Steady blue indicates that service action can be taken on the controller without adverse consequences. Off indicates that the controller is engaged and service action must not be implemented.
<i>Expansion Unit Indicators</i>	
Expansion Port Rate 	The combined display indicates the expansion port link rate for the tray: LED 4 Off, LED 2 On – 2 Gbits/second
Expansion Port Bypass 	Steady amber indicates that no valid device is detected and that the drive port is bypassed. Off indicates that there is no SFP installed or that the port is enabled.

Mixed FC and SATA Capacity

Mixed Serial Advanced Technology Attachment (SATA) and Fibre Channel (FC) configurations are supported with the following restrictions:

- Each controller and expansion unit must contain all FC drives or all SATA drives. Do not mix FC and SATA drives within a controller unit or expansion unit.
- The controller unit can contain FC drives even if one or more expansion units contain SATA drives.

- The controller unit can contain SATA drives even if one or more expansion units contain FC drives.
- Each array (controller unit and connected expansion units) can contain mixed FC and SATA drives. However, because SATA drives are so much slower than FC drives, connect any SATA expansion units at the end.
- In a dual-array configuration, the arrays can be configured differently (different types of drives).
- A unique hot-spare must be available for both SATA and FC in the same capacity as used in the array.
- Logical unit numbers (LUNs) cannot include both SATA and FC drives.
- Expansion units must be at the same firmware level as the RAID controller to which they are connected. For example, if you add an expansion unit at firmware level 1.2 to a RAID controller unit at firmware level 1.0, you must upgrade the entire system to level 1.2.

Disk Drives

Only FC or SATA drives supplied by Sun Microsystems work with the NAS appliances. For the most current support information, contact your Sun sales representative.

Each drive is encased in its own drive shuttle, as illustrated below:

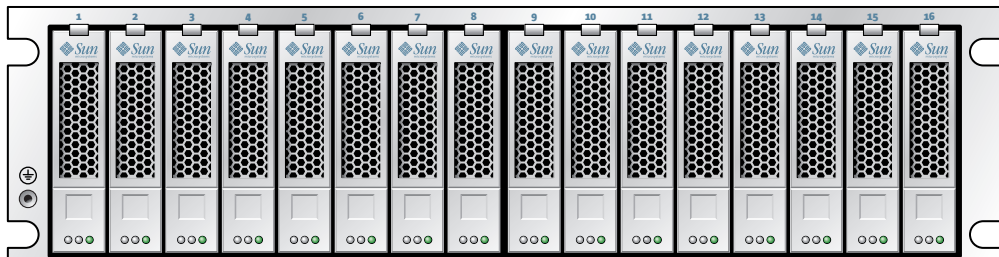


FIGURE D-9 Sun StorageTek 5320 Fibre Channel Drive Shuttles

When a drive is determined to be bad, contact Sun Services to replace the failed drive.

Drive shuttles can be replaced individually, without shutting down the expansion unit, controller unit, or NAS server. As necessary, only hot-swap one drive shuttle at a time. Confirm that the RAID subsystem has completed any necessary rebuild before removing another drive shuttle.

Identifying a Drive for Replacement

If a disk drive fails, use the system log or a diagnostic report to identify the drive. The example below shows an entry from the system log:

```
Controller 1 enclosure 0 row 0 column 6
```

This example references the drive in slot 7 of the first enclosure in the first array. Use the guidelines below to interpret log entries and diagnostic reports. Ignore any channel and target numbers that display in the log (not illustrated above). These are maintained for compatibility with legacy systems.

- Controller numbering starts at 0. The controllers in the first array (that is, the first controller unit) are 0 (slot A) and 1 (slot B), and the controllers in the second array are 2 and 3. The arrays are numbered by the NAS OS when you first start up the system after installation, in order as you boot them. If you follow the recommended power-up sequence, the first HBA port on the server (PCI 1) is connected to the first array (controllers 0 and 1), and the second HBA port (PCI 0) is connected to the second array.
- Enclosure numbering starts at 0 and is relative to the array to which it belongs. For example, if the first array has a controller unit and one expansion unit, they are identified as enclosures 0 and 1. Additional expansion units are numbered in the order in which they were booted when you first started up the system after installing the NAS device. The *Getting Started Guide* details the recommended power-up sequence.
- The row number is always 0.
- Column numbering starts at 0, and identifies the physical position of the drive as you face the controller unit or expansion unit from the front, moving left (column 0) to right (column 15).

Note: The numbering on the physical device (silk screen) runs from 1 to 16, corresponding to columns 0 through 13.

Locating a Drive

To locate a particular drive, see [“Locating a Drive or Controller/Expansion Unit” on page 174](#). This will cause the drive indicator lights to flash for a selected drive.

Sun StorageTek 5220 NAS Appliance

The Sun StorageTek 5220 NAS Appliance is the basic unit. [FIGURE D-1](#) shows the front of the appliance. You need the software serial number for any calls for service and for adding licenses and you need the hardware serial number if you decide to expand the system.

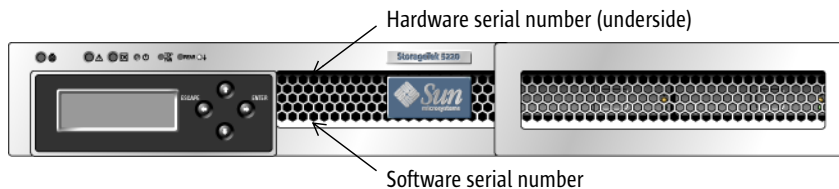


FIGURE D-22 Sun StorageTek 5220 NAS Appliance, Front

[FIGURE D-3](#) shows the back of the appliance. The appliance contains a dual-port fibre channel (F C) host bus adapter (HBA) card in PCI slot 1. The other slot, PCI slot 0, can be empty or contain one of the optional cards.

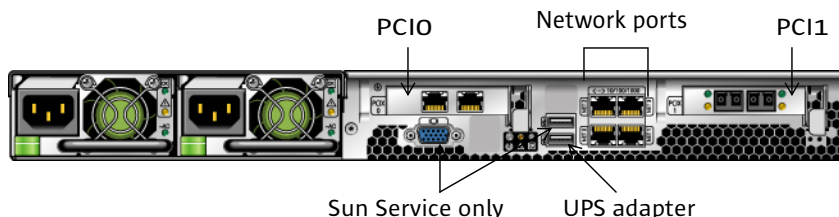


FIGURE 4-23 Sun StorageTek 5220 NAS Appliance With Single HBA Card, Back

One of the ports on the HBA card in PCI slot 1, HBA Port 2, can be used for connecting to tape backup. Its other port, HBA Port 1, is dedicated to connecting to the controller unit.

PCI slot 0 can contain the following options:

- A dual-port copper 10/100/1000 Gigabit Ethernet card
- A dual-port optical Gigabit Ethernet card
- A FC HBA card for tape backup
- A SCSI HBA card for tape backup

An uninterruptible power supply device (UPS), using the USB-to-Serial Port Adapter/Convert Cable included in the ship kit. If a power outage occurs, the UPS maintains the operation of the system. If the battery in the UPS loses power, the UPS performs a graceful shutdown of the system. Connecting the UPS adapter cable to a supported local UPS device enables the appliance to monitor the state of the UPS.

Back-End Storage

The RAID controller unit provides direct-attached back-end storage for the Sun StorageTek 5220 NAS Appliance. At a minimum, the system has an appliance and one controller unit containing SATA disk drives. In addition to the appliance and controller unit, you can set up additional back-end storage by connecting one or two expansion units to the controller unit, as described in [“Expansion Units” on page 332](#). Each expansion unit must contain only SATA disk drives.

Sending a Diagnostic Email Message

The diagnostic email feature enables you to send email messages to the Sun Services team, or any other desired recipient. A diagnostic email message includes a single compressed file, `diag.tar.gz`, containing all of the following information:


- `Diag.txt`, including information about the following:
 - Date and time
 - Uptime
 - CPU %
 - User
 - Software and OS
 - Hardware
 - Disk sub-systems
 - LUN paths
 - Disk error retry count
 - File systems
 - Network
 - Backup and Restore
 - Windows share
 - ADS
 - CIFS
 - Mirroring
 - NTP
 - Environment
 - Enclosures

- System Log
 - Text entered in the Problem Description field
- Configuration and log files from /dvol/etc directory
 - passwd
 - group
 - hosts
 - approve
 - hostgrps
 - users.map
 - group.map
 - partner.log
- Local backup file under backup.directory
- Network capture file: netmdiag.cap.gz
- All files from /cvol/log
 - bootlog
 - dbglog
 - history
 - problem.txt
- RAID information from /dvol/support directory
- All syslog files

Every diagnostic email message sent includes all of this information, regardless of the problem. The same compressed file is stored in the /dvol/diagnostic directory with a maximum two files.

In a cluster configuration, you must set up diagnostic email for each server in the cluster.

To set up diagnostic email in the Web Administrator graphical user interface (GUI):

1. In the toolbar, click the  button.
The Diagnostic Email window is displayed.
2. Type a description of the problem in the Problem Description field.
This is a mandatory entry and is limited to 256 characters.
3. Ensure that the Diagnostics checkbox is selected for at least one email recipient.
If you need to add or make changes to recipients, see "[Setting Up Email Notifications](#)" on page 34.
4. Click Send to send the message.

To set up diagnostic email from the console:

1. From the Extensions menu, choose Diagnostics.
2. Choose 2, Send Email.
3. Choose 1, Edit Problem Description to add text to the message.
This is a mandatory entry and is limited to 256 characters.
4. Choose 8, Send Email

The compressed file is also stored in the default directory, up to a maximum of two versions.

Web Administrator Panels

This appendix lists the fields and elements in the Web Administrator graphical user interface. It includes the following sections:

- [“Add LUN Wizard Panels” on page 346](#)
- [“Antivirus Configuration Panels” on page 350](#)
- [“Configuration Wizard Panels” on page 352](#)
- [“File Replicator Panels” on page 353](#)
- [“File Volume Operations Panels” on page 361](#)
- [“High Availability Panels” on page 378](#)
- [“iSCSI Configuration Panels” on page 382](#)
- [“Monitoring and Notification Panels” on page 387](#)
- [“Network Configuration Panels” on page 398](#)
- [“RAID Panels” on page 408](#)
- [“System Activity Panels” on page 415](#)
- [“System Backup Panels” on page 417](#)
- [“System Manager Panels” on page 418](#)
- [“System Operations Panels” on page 420](#)
- [“Unix Configuration Panels” on page 432](#)
- [“Windows Configuration Panels” on page 443](#)

Within each section, the Web Administrator windows are described in order alphabetically, by name.

Add LUN Wizard Panels

Use the Add LUN wizard to create a new logical unit number (LUN) for Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances and gateway systems. You will create the LUN on an existing redundant array of independent disks (RAID) set, or over previously unallocated drives.

Type the required information in each window and click Next to continue. At the end of the wizard, you can review the information you have entered and then either edit it before saving it, or discard it by clicking Cancel.

Click a link below for information about that panel in the Add LUN wizard:

- [“Select Controller Unit and Drives or RAID Set” on page 346](#)
- [“LUN Properties” on page 349](#)
- [“Confirmation Panel” on page 350](#)
- [“Save Configuration” on page 350](#)

Select Controller Unit and Drives or RAID Set

This panel displays disk drives and redundant array of independent disks (RAID) sets that belong to each controller unit. A RAID set is a set of drives that you logically group together to provide capacity for one or more logical unit numbers (LUNs).

The following table describes the fields and buttons on this panel.

TABLE F-1 Fields and Elements on the Select Controller Unit and Drives or RAID Set Panel

Field	Description
Controller Unit	From the drop-down menu, select the controller unit that will manage the new LUN.
RAID Set	Select an existing RAID set, or click <i>Use unassigned drives and select at least three drives from the graphical image on the right.</i>

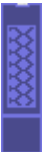






TABLE F-1 Fields and Elements on the Select Controller Unit and Drives or RAID Set Panel (Continued)

Field	Description
Drive Icons	<p>Graphic representation of the drives in the NAS device. If you are using unassigned drives, select three or more drives for the new LUN. The icons reflect the status of each drive, as follows:</p> <ul style="list-style-type: none"> For Sun StorageTek 5320 controller units and expansion units, see TABLE F-2 for a description of the drive-status icons. For Sun StorageTek 5300 controller enclosures and expansion enclosures, see TABLE F-3 for a description of the drive-status icons.

Sun StorageTek 5320 Drive Status Indicators

The Sun StorageTek 5320 drive images show the status of each drive, as described in the following table.





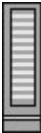


TABLE F-2 Sun StorageTek 5320 Drive Status Indicators (Add LUN)

Drive	Indication
	<p>or</p>  <p>Drive is selected for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).</p>
	<p>or</p>  <p>Drive is available to be selected for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).</p>
	<p>or</p>  <p>Drive is not available for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).</p>
	<p>Drive slot is empty (no drive present).</p>

Sun StorageTek 5300 Drive Status Indicators

The Sun StorageTek 5300 drive images show the status of each drive, as described in the following table.

TABLE F-3 Sun StorageTek 5300 Drive Status Indicators (Add LUN)

Drive	Indication
	or  Drive is selected for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).
	or  Drive is available to be selected for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).
	or  Drive is not available for LUN membership. Drive is empty (left) or partially allocated to another LUN (right).
	Drive slot is empty (no drive present).

LUN Properties

Use this panel to specify the properties for the new LUN, as described in the following table.

TABLE F-4 Fields and Elements on the LUN Properties Panel

Field	Description
<i>New LUN Assignment</i>	
LUN Size	Size of the logical unit number (LUN), from a minimum size of 100 megabytes (MB) to a maximum of the full disk capacity, not to exceed 2 terabytes. If the size is smaller than the actual disk capacity, the remaining capacity is available for new LUNs.
RAID Level	Redundant array of independent disks (RAID) configuration for the LUN (always RAID 5).
Preferred server ID ownership	Applicable with dual-server systems. Unique identifier assigned to this server that will manage the LUN.
Create New File Volume	Select to create the new LUN on the physical drives or RAID set selected, and to create a new file system on that LUN. Specify the name of the new file volume to the right.
Grow Existing File Volume	Select to create a LUN on the physical drives or RAID set selected, and to use that LUN to expand the storage for an existing file system. Select the target file system from the drop-down menu.
None	Select to create the new LUN, but to not create a file system on the LUN.
<i>Drive Icons</i>	Display-only graphic representation of the drives in the NAS device. The drives marked for use by the LUN were configured on the previous panel. The icons reflect the status of each drive, as follows: <ul style="list-style-type: none">• For Sun StorageTek 5320 controller units and expansion units, see TABLE F-2 for a description of the drive-status icons.• For Sun StorageTek 5300 controller enclosures and expansion enclosures, see TABLE F-3 for a description of the drive-status icons.

Confirmation Panel

This panel displays a summary of the settings for the new LUN (logical unit number). Review the settings to make sure they are accurate, then click Finish to create the LUN.

The right side of the panel shows a graphic representation of the drives in the NAS device. The icons reflect the status of each drive, as follows:

- For Sun StorageTek 5320 controller units and expansion units, see [TABLE F-2](#) for a description of the drive-status icons.
- For Sun StorageTek 5300 controller enclosures and expansion enclosures, see [TABLE F-3](#) for a description of the drive-status icons.

Save Configuration

This panel displays the status as the logical unit number (LUN) is created.

Antivirus Configuration Panels

This section describes the fields and elements on the Configure Antivirus panel.

Configure Antivirus Panel

This panel enables you to configure antivirus software for the system.

The following table describes the fields and buttons on this panel.

TABLE F-5 Fields and Elements on the Configure Antivirus Panel

Field	Description
Enable Antivirus	Select to enable antivirus protection for NAS files.

TABLE F-5 Fields and Elements on the Configure Antivirus Panel (*Continued*)



Field	Description
Scan Engine IP Address	Internet Protocol (IP) address of the system that is running the scan engine software you want to use. You can specify up to four scan-engine systems.
Port #	Number of the port, on the scan-engine PC, through which the scan engine listens for scan requests. This is typically port 1344.
Max Conn	Maximum number of concurrent file scan operations (connections) the scan engine can support from the NAS device. This defaults to two, but is typically set higher.
Delete buttons 	The panel contains two Delete buttons: one removes a scan engine from operation and one removes a file type from a list of file types. To remove a scan engine, select it and then click the Delete button. To remove a file type from the list of included file types or the list of excluded file types, select the file type and then click the Delete button.
Options	Options that limit the file size for antivirus scan processing
• Max Scan Size	Specifies the maximum size of file that can be sent to the scan engine for scanning. The file size can be specified as 1 to 1023 KB, MB, or GB.
• Access	Specifies the action to be taken if the specified size limit is exceeded.
Type	File types that you want scanned or ignored by the antivirus software. For each file type, specify its value in the List field and then click the Add button. <ul style="list-style-type: none"> • File Types Included - Types of files to be scanned by the antivirus software, specified as a 1-to-4 character file extension. If no types are listed, <i>all</i> types are scanned. If any types are listed, <i>only</i> the listed types are scanned. File types are case insensitive, and support * and ? wildcard matching. <p>Note: If a file type is listed as both included and excluded, it is <i>excluded</i>.</p> • File Types Excluded - Types of files to be ignored by the antivirus software, specified as a 1-to-4 character file extension. File types are case insensitive, and support * and ? wildcard matching.
List	File types that you want scanned or ignored by the antivirus software. Enter new types in the field at the top of the list, then click the Add button to add that object to the full list, which displays below it.
Add button 	Confirms that a new file type is added to the full list.
Apply	Click to save your changes.

TABLE F-5 Fields and Elements on the Configure Antivirus Panel (*Continued*)

Field	Description
Cancel	Click to clear the fields of new entries and close out of the window without saving your entries.

Configuration Wizard Panels

This section describes the fields and elements on the Configuration Wizard panels:

- [“Configuration Wizard Panel” on page 352](#)
- [“Confirmation Panel” on page 352](#)
- [“Select Environment Panel” on page 353](#)

Configuration Wizard Panel

This is the first screen of the configuration wizard. The configuration wizard is a tool that enables you to configure newly attached systems by entering information in a series of windows.

Type the required information in each window and click Next to continue. At the end of the wizard, you can review the information you have entered and then either edit it before saving it, or discard it by clicking Cancel.

Confirmation Panel

This panel is the last screen of the configuration wizard. It enables you to confirm or discard the information you have entered in the configuration wizard.

Perform one of the following in this window:

- To change the information you have entered before saving it to the system:
 - a. Click the Back button to return to the window in which you want to make changes.
 - b. Make your changes and click Next to return to the Confirmation panel.
 - c. Click Finish.

Your changes are saved to the system.

- To save the configuration information that you have entered in the system, click Finish.
- To close out of the configuration wizard without saving any information, click Cancel.

Select Environment Panel

This panel enables you to configure the network environment for your newly attached system.

The following table describes the fields and buttons on this panel.

TABLE F-6 Fields and Elements on the Select Environment Panel

Field	Description
<i>Network</i>	
Configure for Windows Only Networks	Select to set a Windows-only network for the system. Select this option if you have no Unix servers on your network.
Configure for Unix Only Networks	Select to set a Unix-only network for the system. Select this option if you have no Windows servers on your network.
Configure Both Windows and Unix Networks	Select to set a mixed Windows and Unix network for the system. Select this option if you have both Windows and Unix servers on your network.

File Replicator Panels

This section describes the fields and elements on the File Replicator panels:

- [“Add/Edit Mirror Window” on page 354](#)
- [“Manage Mirrors Panel” on page 355](#)
- [“Promote Volume Window” on page 356](#)
- [“Set Threshold Alert Panel” on page 357](#)
- [“View Mirror Statistics Panel” on page 358](#)

Add/Edit Mirror Window

This window enables you to add or edit a mirror, depending on whether you accessed the window by clicking Add or Edit.

The following table describes the fields and buttons in this window.

TABLE F-7 Fields and Elements on the Add/Edit Mirror Window

Field	Description
Volume	Select the file volume you want to mirror. This field is editable only if the window is in Add mode.
Mirror Host	Name of the server that hosts the mirrored file volume. This field is editable only if the window is in Add mode.
IP Address	Internet Protocol (IP) address to be used for the mirror connection. It is recommended that you use a private network link for mirroring (a link that is not accessible to other devices in the network).
Alternative IP Address	(Optional) IP address that will be used to maintain the mirror in the event that the first IP address becomes unavailable.
Password	Enter the system administrator password of the remote host.
Mirror Buffer Size (MB)	Available only if the window is in Add mode. Size of the mirror buffer, in megabytes (MB). The mirror buffer stores file-system write transactions while they are being transferred to the mirror host server. The size of the mirror buffer depends on a variety of factors, but it must be at least 100 MB and must be at least several gigabytes in size. You might want to create a mirror buffer that is approximately 10% of the size of the mirrored file volume. The size you specify is more a function of the write activity to the source file volume than it is of the file volume size. It is important to note that the file volume free space on the active server will be reduced by the allocation size of the mirror buffer.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving your entries.

Manage Mirrors Panel

This panel enables you to add, edit, or break mirrors between the active server and the mirror server. After a mirror has been broken on the active server, the mirrored file volume can be promoted, or made available for users, on the mirror server.

Note: If a file volume is compliance enabled, you cannot promote the file volume.

The following table describes the fields and buttons on this panel.

TABLE F-8 Fields and Elements on the Manage Mirrors Panel

Field	Description
Volume	File volume being mirrored.
Active Server	Name or IP address of the server on which the file volume originally exists.
Mirror Server	Name or IP address of the server that is hosting the mirrored file volume.
Sync Status	Status of the mirror: <ul style="list-style-type: none">• New – A new mirror is being created.• Creating mirror log – The mirror buffer is being initialized.• Connecting to host – The active server is connecting to the remote mirror server.• Creating extent – Disk partitions are being created on the mirror server.• Ready – The system is ready and waiting for the other system to be ready.• Down – The network link is down.• Cracked – The mirror is cracked.• Syncing Volume – The file volume is being synchronized on the mirror server. There can be no I/O activity to the mirror volume during this process. The volume is taken offline to avoid transient file system errors and inconsistencies.• In Sync – The mirror is in sync.• Out of Sync – The mirror is out of sync.• Error – An error has occurred.• Mirror is out of space – The mirror has no more space available for storage use.• Initializing Mirror Buffer <i>percent-complete</i> – The mirror showed signs of cracking and is replicating itself. The mirror file volume will go off-line until the <i>percent-complete</i> reaches 100%.

TABLE F-8 Fields and Elements on the Manage Mirrors Panel (*Continued*)

Field	Description
New	(Active server only) Click to mirror a file volume from the active server to the mirror server.
Break	Click to break the selected mirror. You can break a mirror volume from the active server or mirror server.
Edit	(Active server only) Click to edit the selected mirror.
Promote	(Mirror server only) Click to launch the Promote Volume window from which you can select the file volume located on the mirror server that you want to promote. Note: You can only promote a mirror that has already been broken on the active server.
Change Roles	Click to enable the active volume to function as the mirror volume and vice versa. This does not change the original configuration on each volume. To change the mirror volume role, select the file volume and click Change Roles.

Promote Volume Window

This window enables you to promote a mirrored volume (make it available for users) on the mirror server. When you promote a volume, the original volume is treated as a separate volume. The promoted volume will no longer be associated with the original volume.

The following table describes the fields and buttons on this panel.

TABLE F-9 Fields and Elements on the Promote Volume Window

Field	Description
Available Volumes	Select the volume to be promoted.
Rename volume after promoting?	Select to rename the volume.
New Name	(Optional) Specify a new name for the volume, if you wish to change the name of the promoted volume. The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 12 alphanumeric characters (a-z, A-Z, 0-9).
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Set Threshold Alert Panel

This panel enables you to set the threshold alert for all mirrored file volumes. The threshold alert is the percentage of mirror buffer usage at which a warning is sent to designated recipients.

The mirror buffer stores file-system write transactions while they are being transferred to the mirror host server. Increases in write activity to the active server or a damaged network link can cause the transference of write transactions to the mirror server to become backed up in the mirror buffer. If the mirror buffer becomes overrun in this process, the mirror will be cracked and no further transactions will occur between the active server and the mirror server until the mirror is reestablished.

To prevent this situation, the software sends warnings when the mirror buffer is filled to certain threshold percentages.

The following table describes the thresholds and buttons on this panel.

TABLE F-10 Fields and Elements on the Set Threshold Alert Panel


Field	Description
	Click and drag this icon to move the threshold value along the scale. As you move the icon, the threshold value that is displayed on the right is updated.
Mirroring Buffer Threshold 1 (%)	The percentage of mirror buffer usage that triggers the first alert. The default value is 70%. This means that when the mirror buffer is 70% full, an alert will be issued.
Mirroring Buffer Threshold 2 (%)	The percentage of mirror buffer usage that triggers the second alert. The default value is 80%.
Mirroring Buffer Threshold 3 (%)	The percentage of mirror buffer usage that triggers the third alert. The default value is 90%.
Alert Reset Interval (Hours)	The amount of time the software will wait before re-issuing an alert that it has already issued. For example, if you set the Mirroring Buffer Threshold 1 to be 10% and the Alert Reset Interval to two hours, the first alert will be issued when the mirror buffer is 10% full. The software will not issue the Threshold 1 alert again for the next two hours. If at that time the mirror buffer usage is still beyond the 10% threshold, the Threshold 1 alert will be issued again. The default value is 24 hours.
Apply	Click to save your changes.

TABLE F-10 Fields and Elements on the Set Threshold Alert Panel (*Continued*)

Field	Description
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

View Mirror Statistics Panel

This panel enables you to view network statistics for mirrored file volumes.

The following table describes the thresholds and buttons on this panel.

TABLE F-11 Fields and Elements on the View Mirror Statistics Panel

Field	Description
<i>Select Volume</i>	
List of Volumes	Select the mirrored file volume for which you would like to see network statistics.
Status	A line of text that describes the status of the mirror.
<i>Transactions (transactions/second)</i>	
Incoming	The incoming transaction statistics for the selected volume, in terms of transactions per second: <ul style="list-style-type: none">• Avg - The average number of transactions per second traveling into the active server.• Min - The lowest number of transactions per second that has traveled into the active server. The date and time that this number of transactions occurred is shown on the right, if available.• Max - The largest number of transactions per second that has traveled into the active server. The date and time that this number of transactions occurred is shown on the right, if available.

TABLE F-11 Fields and Elements on the View Mirror Statistics Panel *(Continued)*

Field	Description
Outgoing	<p>The outgoing transaction statistics for the selected volume, in terms of transactions per second:</p> <ul style="list-style-type: none"> • Avg - The average number of transactions per second traveling from the active server to the mirror server. • Min - The lowest number of transactions per second that has traveled from the active server to the mirror server. The date and time that this number of transactions occurred is shown on the right, if available. • Max - The largest number of transactions per second that has traveled from the active server to the mirror server. The date and time that this number of transactions occurred is shown on the right, if available.
<i>Mirror Buffer (transactions)</i>	
Size	The size of the mirror buffer, in terms of transactions (not bytes).
Free	The number of transactions left in the mirror buffer.
Utilization	<p>The percentage of mirror buffer that is currently being used to hold transactions. If this value approaches 100%, check to make sure that all network links are functioning properly. In the event that a network link goes down, the buffer will be filled up and eventually overrun. This means that transactions are travelling into the active system faster than they are travelling into the mirror system, filling up the buffer. When the buffer is overrun, the mirror has been cracked.</p> <p>After the network link is repaired, the system will begin the mirror update process until the mirrored file volume is back in sync. There can be no I/O activity to the mirror volume during the resync. The volume is taken offline to avoid transient file system errors and inconsistencies.</p>
Fill Rate	<p>The rate at which the mirror buffer is filling, transactions per second. If the fill rate is greater than zero, check that all network links are functioning properly. If a network link is disabled, transactions travel into the active system faster than they are travelling into the mirror system, filling up the buffer. If the buffer is overrun, the mirror has been cracked.</p> <p>After the network link is repaired, the system begins the mirror update process until the mirrored file volume is back in sync. There can be no I/O activity to the mirror volume during the resync. The volume is taken offline to avoid transient file system errors and inconsistencies.</p>
<i>Network Statistics</i>	
<i>Host</i>	

TABLE F-11 Fields and Elements on the View Mirror Statistics Panel (*Continued*)

Field	Description
Hostname	The name of the host, recognized by the network, that will be used for the mirror buffer.
Connected	A line of text that indicates how the host being used by the mirror buffer is connected to the network.
Connected Since	The date on which the host that is being used by the mirror buffer was first connected to the network.
<i>Link</i>	
Status	The link status of the mirror buffer on the network.
Link Quality	The quality of the mirror buffer link on the network.
Errors	Any errors associated with the mirror buffer link on the network.
Timeouts	The number of timeouts for the mirror buffer link on the network.
Drops	The number of drops for the mirror buffer link on the network.
Time of Last Transfer	The time and date at which the last transfer of memory buffer over the network occurred.
<i>Request Control Blocks</i>	
Sent	The number of control blocks sent across the network by the memory buffer.
Total Bytes	The total bytes of control blocks sent across the network by the memory buffer.
Average Size	The average size of the memory buffer control blocks.
Rate	The rate, per second, of control blocks sent across the network by the memory buffer.
<i>Transfer Rate</i>	
Average (kb/s)	The average rate, in terms of kilobytes per second, at which transfers occur for the memory buffer.
Max (kb/s)	The largest amount of transfers, in terms of kilobytes per second, that occurred for the memory buffer across the network.
When Max Occurred	The date and time when the maximum transfers occurred.
<i>Response Time</i>	
Average (msec)	The average response time of the memory buffer.
Max (msec)	The highest response time of the memory buffer.
When Max Occurred	The date and time at which the highest response time occurred.

File Volume Operations Panels

This section describes the fields and elements on the File Volume Operations panels:

- [“Add/Edit Checkpoint Schedule Window” on page 361](#)
- [“Add/Edit DTQ Setting Window” on page 362](#)
- [“Add/Edit Quota Setting Window” on page 363](#)
- [“Attach Segments Panel” on page 365](#)
- [“Configure Directory Tree Quotas Panel” on page 365](#)
- [“Configure User and Group Quotas Panel” on page 366](#)
- [“Create Checkpoint Window” on page 368](#)
- [“Create File Volumes/Segments Panel” on page 369](#)
- [“Delete File Volumes Panel” on page 370](#)
- [“Edit Volume Properties Panel” on page 371](#)
- [“Manage Checkpoints Panel” on page 373](#)
- [“Rename Checkpoint Window” on page 373](#)
- [“Schedule Checkpoints Panel” on page 374](#)
- [“Segment Properties Window” on page 376](#)
- [“View Volume Partitions Panel” on page 377](#)

Add/Edit Checkpoint Schedule Window

This window enables you to add or edit a checkpoint schedule, depending on whether you accessed the window by clicking Add or Edit.

Note: A large amount of space and system memory is required for checkpoints. The more checkpoints there are on a system, the greater the effect on system performance.

The following table describes the fields and buttons in this window.

TABLE F-12 Fields and Elements on the Add/Edit Checkpoint Schedule Window

Field	Description
Volume	The volume for which you want to create or edit a checkpoint schedule. If you are editing the checkpoint schedule, you cannot select a different volume from this list.

TABLE F-12 Fields and Elements on the Add/Edit Checkpoint Schedule Window

Field	Description
Description	A line of text that describes the checkpoint. This is a mandatory field.
Keep Days + Hours	The period of time (number of days plus number of hours) for which the checkpoint will be retained after being created. In the Days box type an integer value between 0 and 99. From the Hours drop-down menu, select an integer value between 0 and 23. This is a mandatory field.
Days	The days on which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional days.
AM Hours	The morning hours at which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional items.
PM Hours	The evening hours at which the checkpoint is to be created. To select more than one item in this list, hold down the Ctrl key while clicking additional items.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit DTQ Setting Window

This window enables you to create or edit a directory in the file system and configure a quota for it.

The following table describes the fields and buttons in this window.

TABLE F-13 Fields and Elements on the Add/Edit DTQ Setting Window

Field	Description
DTQ Name	Name used to identify this directory tree quota. The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 30 alphanumeric characters: a-z, A-Z, 0-9 and underscores (_).
Dir Name	Name for the new directory. Directory quotas can only be configured for directories created in this field.

TABLE F-13 Fields and Elements on the Add/Edit DTQ Setting Window (Continued)

Field	Description
Path	<p>If you get access to this panel from the System Manager window, the Path field is read-only.</p> <p>If you get access to this panel from the Configure Directory Tree Quotas window, you can populate the Path field and add a directory tree quota.</p> <p>Click the folders in the box below the Path field to populate the Path field. The box shows the directory tree structure for the file volume on which the directory will reside. To view the contents of a folder in this box, click the symbol next to the folder, or double-click the folder itself. Then select the directory that will contain the new directory for which you are setting this quota.</p>
Disk Space Limits	<p>Disk space limit for the directory, between No Limit and Custom:</p> <ul style="list-style-type: none">• No Limit - Select to enable unlimited disk space usage for the directory.• Custom - Select to designate a maximum amount of disk space that can be used on the directory. Specify whether the quota is to be determined in megabytes or gigabytes, and type the disk space limit in the Max Value field. Typing a value of 0 (zero) is equivalent to choosing No Limit.
File Limits	<p>Maximum number of files that can be written to this directory, between No Limit and Custom.</p> <ul style="list-style-type: none">• No Limit - Select to enable an unlimited number of files to be written to this directory.• Custom - Select to designate a maximum number of files that can be written to this directory. Then type the file limit in the Max Value field.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit Quota Setting Window

This window enables you to add or edit user or group quotas, depending on how you accessed the window (by clicking Add or Edit). Quotas designate disk space and file limits for NT and Unix users and groups.

The following table describes the fields and buttons in this window.

TABLE F-14 Fields and Elements on the Add/Edit Quota Setting Window

Field	Description
Volume	Volume for which you are adding or editing a user or group quota.
User/Group	User or group for which you are adding or editing a quota. If you are adding a quota, specify whether the designated user or group belongs to a Unix or Windows environment by selecting the appropriate Unix or Windows radio button. Then select the user or group name (and Domain name, for NT users/groups) from the corresponding drop-down menus.
Disk Space Limits	Disk space limits for the selected user or group. Select one of the following: <ul style="list-style-type: none">• Default – Select to set the hard and soft limits to be the same as that of the default user or group, as shown in the “Configure Directory Tree Quotas Panel” on page 365.• No Limit – Select to enable unlimited space usage by the user or group.• Custom – Select to define soft and hard limits for the user or group. Specify whether the quota will be designated in kilobytes, megabytes, or gigabytes. Then type the maximum amount of disk space usage for the user or group in the Max Value field.
File Limits	Maximum number of files a user or group can write to the selected volume. Select one of the following: <ul style="list-style-type: none">• Default – Select to set the hard and soft limits to be the same as that of the default user or group, as shown in the “Configure Directory Tree Quotas Panel” on page 365.• No Limit – Select to enable an unlimited number of files to be written by the user or group.• Custom– Select to define soft and hard limits for the user or group. Specify whether the quota will be designated in kilobytes, megabytes, or gigabytes. Then type the maximum number of files to be written by the user or group in the Max Value field.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Attach Segments Panel

You can attach segments to the selected primary volume on the Create File Volumes panel or by right-clicking a System Manager object and choosing the appropriate attach segments menu option.

This window or panel enables you to attach segments to an existing primary file volume. Only one segment can be attached at a time.

Note: After a segment is attached, it cannot be detached from a primary file volume. Instead, it becomes a permanent part of that volume.

The following table describes the fields and buttons on this panel.

TABLE F-15 Fields and Elements on the Attach Segments Panel

Field	Description
Existing Volumes	Click an existing volume to which you want to attach segments. This field is available only from the Create File Volumes panel.
Available Segments	A list of the existing file segments (name, logical unit number (LUN), size (in megabytes) that are available to be attached to primary volumes. If no segments exist, you can create a segment on the “Create File Volumes/Segments Panel” on page 369 . For more information, see “Creating a File Volume or Segment Using the Create File Volumes Panel” on page 51 .
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Directory Tree Quotas Panel

This panel enables you to administer quotas for specific directories in the NAS file system. Directory tree quotas determine how much disk space is available for a directory, and how many files can be written to it.

Note: Quotas can only be created and configured for directories that you create from this panel, not for previously existing directories.

The following table describes the fields and buttons on this panel.

TABLE F-16 Fields and Elements on the Configure Directory Tree Quotas Panel

Field	Description
Volume	Select a primary volume for which you want to configure a directory tree quota.
DTQ Name	The name of the directory tree quota that is applied to a directory on the selected volume.
Max Size (MB)	The largest amount of disk space that can be used in the directory, in megabytes.
Size Used (%)	The percentage of disk space that is currently being used in the directory.
Max File	The largest number of files that can be written to the directory.
File Used	The number of files that are currently written to the directory.
Path	The full path of the directory on the selected volume.
Refresh	Click to update the panel with the latest information about the selected volume.
New	Click to launch the Add DTQ Setting window. From this window, you can create a new directory on the selected volume and can apply a new directory tree quota to that directory.
Edit	Click to launch the Edit DTQ Setting window. From this window, you can edit the selected directory tree quota.
Delete	Click to delete the selected directory tree quota from the table.

Configure User and Group Quotas Panel

This panel enables you to administer user and group quotas on volumes for NT and Unix users and groups. User and group quotas determine how much disk space is available to a user or group, and how many files a user or group can write to a volume. Before setting user or group quotas, you must enable quotas for the selected volume on the [“Edit Volume Properties Panel” on page 371](#).

The table displays root, default, and individual quotas for the selected volume. By default, the root user and root group have no hard or soft limits for space or files. The settings for default user and default group are the settings for all users who do not have individual quotas set. For more information about quota limits, see [“About Configuring User and Group Quotas” on page 122](#).

Note: If you want to use user and group quotas, it is recommended that you set up a default disk space or file limit before allowing user or group access. This ensures that users and groups cannot write more data or files than allowed before you configure specific user or group quotas.

The following table describes the fields and buttons on this panel.

TABLE F-17 Fields and Elements on the Configure User and Group Quotas Panel

Field	Description
Volume	Select an existing volume for which you want to create a user or group quota.
Users	Select to display existing user quotas that are applied to the selected volume.
Groups	Select to display existing group quotas that are applied to the selected volume.
ID	The unique identifier assigned to the user or group quota.
Name	The name of the user or group quota.
Windows Name	The name of the user or group quota as recognized by the Windows environment.
KB Used	The amount of disk space that is currently being used on the volume by the user or group.
Soft KB Limits	A value, equal to or lower than the Hard KB Limits value, that triggers a grace period of seven days. After this grace period is over, the user or group cannot use any more disk space on the volume until the amount of consumed disk space is below the soft limit.
Hard KB Limits	A value, equal to or higher than the Soft KB Limits value, that determines the maximum amount of disk space that can be used on the selected volume by the user or group.
KB Limits Grace	If kilobytes are in excess of soft block quota, the time remaining in the seven-day grace period. Field is blank if the user is within soft quota.
Files Used	The number of files that have been written to the selected volume by the user or group.
Soft File Limits	A value, equal to or lower than the Hard File Limits value, that triggers a grace period of seven days. After this grace period is over, the user or group cannot write any more files to the volume until the number of files already written to the volume is below the soft limit.
Hard File Limits	A value, equal to or higher than the Soft File Limits value, that determines the maximum number of files that can be written to the volume by the user or group.
File Limits Grace	If currently in excess of soft files quota, time remaining in the seven-day grace period. Field is blank if user is within hard quota.

TABLE F-17 Fields and Elements on the Configure User and Group Quotas Panel

Field	Description
New	Click to launch the New Quota Settings window. From this window, you can create a new user or group quota for the selected volume.
Edit	Click to launch the Edit Quota Settings window. From this window, you can edit the selected user or group quota.

Create Checkpoint Window

This window enables you to create a checkpoint.

The following table describes the fields and buttons in this window.

TABLE F-18 Fields and Elements on the Create Checkpoint Window

Field	Description
Volume Name	Volume for which you want to create or edit a checkpoint (display-only).
Auto Delete	Select to enable the system to assign a name to the checkpoint, and to remove the checkpoint after the time specified in Keep Days and Hours has elapsed. Specify the following: Keep Days + Hours - The number of days and hours the checkpoint will be retained. In the Days field, type an integer value between 0 and 99. From the Hours drop-down menu, select an integer value between 0 and 23.
Manual	Select to always retain the checkpoint until it is manually deleted. In the Name field, specify the name by which the checkpoint will be saved. The name can include any alphanumeric characters except a slash (/), and can be up to 23 characters in length.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Create File Volumes/Segments Panel

You create a volume or segment by using the Create File Volumes panel or by right-clicking on the System Manager from the navigation panel and then choosing the appropriate menu option.

You can create a maximum of 31 file volumes for each logical unit number (LUN). A single file volume is limited to 256 gigabytes. However, you can create a larger volume by attaching segments to a primary volume. You can attach up to 63 segments.

Before creating a file volume of segments, scan for disks that might have been added to the system recently. To perform this scan, do one of the following:

- From the navigation panel, right-click System Manager and choose Scan for New Disks.
- From the navigation panel, choose File Volume Operations > Create File Volumes and select Scan for New Disks.

The following table describes the fields and buttons on this panel.

TABLE F-19 Fields and Elements on the Create File Volumes/Segments Panel

Field	Description
LUN	Click the logical unit number (LUN) on which you want to create a file volume or segment. A maximum of 31 file volumes can be created for each LUN. Clicking on a LUN updates the graphic image, which shows how the LUN is configured, as described in the Legend section.
Name	The name of the file volume or segment. The name must begin with a letter of the alphabet (a-z, A-Z), and can contain up to 12 alphanumeric characters (a-z, A-Z, 0-9). You cannot name a file volume of the Raw type. The Raw type of volume always has the name "raw" and is limited to one for each LUN.
Partition	If partitions exist, select the partition on which you want to create a file volume or segment. If they do not exist, you can use the Initialize Partition Table button to create 31 partitions.
Size	Enter the size of the new file volume or segment. From the drop-down menu, select either megabytes (MB) or gigabytes (GB).
Type	This field is available only on the File Volume Operations > Create File Volumes panel. Select the type of partition: Primary, Segment, or Raw.
Virus Scan Exempt	Select to exempt the file volume from antivirus scan.

TABLE F-19 Fields and Elements on the Create File Volumes/Segments Panel *(Continued)*

Field	Description
Compliance Archiving	This field is available only if you are creating a file volume on a primary partition and you are on the File Volume Operations > Create File Volumes panel. Click to enable the compliance and then click either a mandatory or advisory compliance enforcement volume. Mandatory compliance volumes cannot be deleted.
Legend	Identifies the colors used in the graphic image of the selected LUN: <ul style="list-style-type: none"> • Orange - Indicates the primary partition on the LUN. • Light Blue - Indicates the segmented partition on the LUN. • Green - Indicates the file-volume mirror (applicable when the Sun StorageTek File Replicator option is licensed and enabled). • Blue - Indicates that the DOS read-only attribute is applied to the LUN. This DOS read-only attribute is only used on the flash disk for the system volume. • White - Indicates the free space on the LUN. • Brown - Indicates the raw partition on the LUN, if any.
Scan for New Disks	This button is available only if you are on the File Volume Operations > Create File Volumes panel. Click to find disks that have been added to the system.
Initialize Partition Table	Click to create 31 partitions in the LUN, if they do not already exist.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Delete File Volumes Panel

This panel enables you to delete the selected file volume from the configuration.

Note: If the volume is a mandatory compliance volume, it cannot be deleted.

The following table describes the fields and buttons on this panel.

TABLE F-20 Fields and Elements on the Delete File Volumes Panel

Field	Description
Name	The name of the volume that you want to delete.

TABLE F-20 Fields and Elements on the Delete File Volumes Panel (Continued)

Field	Description
LUN	The logical unit number (LUN) on which the volume resides. If the volume is made from multiple partitions that reside in multiple LUN. In this situation, the table lists all LUN/partition pairs.
Partition #	The LUN partition on which the volume resides. The volume might reside on multiple partitions that reside in multiple LUNs. In this situation, the table lists all LUN/partition pairs.
Size (MB)	The size of the volume, in megabytes.
Apply	Click to delete the selected volume.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Edit Volume Properties Panel

This panel enables you to edit the properties of a volume, such as its name, checkpoint option, and quota option.

Note: Compliance volumes cannot be renamed or have their compliance feature disabled. Raw volumes cannot be renamed or have their properties changed.

The following table describes the fields and buttons on this panel.

TABLE F-21 Fields and Elements on the Edit Volume Properties Panel

Field	Description
Volumes	Click the volume that you want to edit.
Volume Name	The name of the selected volume.
New Name	New name of the selected volume (applicable if you wish to change the name). The name must begin with a letter of the alphabet (a-z, A-Z), and can contain up to 12 alphanumeric characters (a-z, A-Z, 0-9).
Virus Scan Exempt	Select to exempt the volume from antivirus scan.
Enable Checkpoints	Click to enable checkpoints for the volume. You must select this box if you plan to maintain file-volume checkpoints, or to run NDMP backups. For information about creating checkpoints, see “About File-System Checkpoints” on page 176. Note: If you clear this checkbox, any checkpoints taken already will be deleted immediately, regardless of their defined retention.

TABLE F-21 Fields and Elements on the Edit Volume Properties Panel (Continued)

Field	Description
Checkpoint Configuration	Options that configure checkpoint processing: <ul style="list-style-type: none">• Use for Backups - Select if you plan to create NDMP backups for the file volume. NDMP performs backups from a copy of the file volume, thereby avoiding potential problems that can occur when working with live data. The backup checkpoint will be deleted immediately after finishing the backup.• Automatic - Select to create and remove checkpoints based on a user-configured schedule.
Enable Quotas	Click to enable quotas for the selected volume.
Enable Attic	Click to temporarily save deleted files in the <code>.attic\$</code> directory located at the root of the 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, disable the <code>.attic\$</code> directory by deselecting this option.
Compliance Archiving	These options are available only if you enabled the advisory compliance enforcement version of the compliance archiving software when you created the volume. Options that enable you to configure compliance archiving software: <ul style="list-style-type: none">• Enabled - An indicator of whether the volume has compliance archiving software enabled.<ul style="list-style-type: none">• Mandatory (No Administrator Override) - The volume is mandatory compliant. You cannot configure this volume to be advisory compliant.• Advisory (Allow Administrator Override) - The volume is advisory compliant. If you want to enable mandatory compliance, you must upgrade to the Mandatory Compliant version of the software, and this is a one-time event.• Default Retention Period - Click to specify how long WORM (write once, read many) files will be retained on the volume if the client does not provide a retention time. The default retention period for a volume is used if a retention period is not applied to a file before that file is retained. Changing the default retention period for a volume does not affect files that have already been retained.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Manage Checkpoints Panel

This panel enables you to view existing checkpoints (one line per checkpoint, per volume), create new checkpoints, and edit and remove existing checkpoints.

The following table describes the fields and buttons on this panel.

TABLE F-22 Fields and Elements on the Manage Checkpoints Panel

Field	Description
Volumes	List of volumes defined. Click a volume to view a list of checkpoints.
Status	Number of checkpoints for the selected volume, and the kilobytes used to store the checkpoints. For example, 1/256 checkpoints, 12K bytes used.
Name	Checkpoint name.
Creation Date	Date when the checkpoint was created.
Expiration Date	Date when the checkpoint will be deleted.
Create	Click to launch the Create Checkpoint window. From this window, you can create a new checkpoint for the selected volume.
Remove	Click to delete the selected checkpoint.
Rename	Click to launch the Rename Checkpoint window, used to edit the name of the selected checkpoint.

Rename Checkpoint Window

This window enables you to rename the selected checkpoint.

Note: If you rename a scheduled checkpoint, it will be marked as a manual checkpoint, and it will not be deleted automatically by the NAS software.

The following table describes the fields and buttons in this window.

TABLE F-23 Fields and Elements on the Rename Checkpoint Window

Field	Description
Volume Name	The name of the volume for which this checkpoint was created. You cannot edit this field.
Old Name	The name of the checkpoint. You cannot edit this field.
New Name	The new name that you want to assign to the checkpoint. The name can include any alphanumeric characters except a slash (/), and can be up to 23 characters in length.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Schedule Checkpoints Panel

This panel enables you to schedule the creation of checkpoints for existing file volumes. You can also view, edit, and remove existing checkpoint schedules. For each checkpoint, this panel displays the volume name, a description, the scheduled checkpoint times and days and the amount of time for which the checkpoint will be retained.

The following table describes the fields and buttons on this panel.

TABLE F-24 Fields and Elements on the Schedule Checkpoints Panel

Field	Description
Volume	A list of all volumes on the system. The first one is selected by default.
<i>Current Checkpoints</i>	A table of existing checkpoints
Description	A line of text that identifies the checkpoint for the selected volume.
Days	The days on which the checkpoint runs.
AM Hours	The morning hours at which the checkpoint runs.
PM Hours	The afternoon and evening hours at which the checkpoint runs.
Keep	The period of time (number of days plus number of hours) for which the checkpoint is to be retained.

TABLE F-24 Fields and Elements on the Schedule Checkpoints Panel (*Continued*)

Field	Description
New	Click to launch the New Checkpoint Schedule window. From this window, you can create a new checkpoint schedule for a volume.
Remove	Click to remove a checkpoint. Select the checkpoint to highlight it and then click the Remove button.
Edit	Click to launch the Edit Checkpoint Schedule window. Select the checkpoint to highlight it and then click the Edit button.
<i>Schedule</i>	A grid of seven days and 24 hours with a checkmark in the cell for each scheduled checkpoint. If you select a checkpoint in the checkpoint table to highlight it, the same checkpoint is highlighted in this grid. If more than one checkpoint is scheduled for the same time, it is displayed in a warning color. This grid is read-only.
<i>Detailed Schedule</i>	A grid of seven days and 24 hours with the retention period of the checkmark in the cell for each scheduled checkpoint. This is the same information as in the Keep field. This grid is read-only.
<i>Forecast Active</i>	A grid of days of the week and number of checkpoints to show the number of active checkpoints on any given time. When you roll the mouse over a portion of the grid, the specific day and number of active checkpoints is displayed. The arrow keys change the display to the previous or next week.

New / Edit Checkpoint Schedule Panel

This panel enables you to create a new checkpoint schedule or change an existing checkpoint schedule for file volumes. Use this panel a description of the checkpoint, the times and days for the checkpoint schedule, and the amount of time for which the checkpoint is retained.

The following table describes the fields and buttons on this panel.

TABLE F-25 Fields and Elements on the New/Edit Checkpoints Schedule Panel

Field	Description
	<p>A grid of seven days and 24 hours with a checkmark in the cell for each scheduled checkpoint for the current file volume.</p> <p>To create a checkpoint: Click on the cell for the day and time for the new checkpoint. The background color of the cell changes and a checkmark symbol is displayed in the cell. If the cell is gray and does not change when you click, an existing checkpoint is overlapping that time.</p> <p>To edit a checkpoint: Click on the cell that shows the checkmark for the checkpoint you want to change. The information for that checkpoint is displayed in the Description and Keep fields.</p>
Description	Enter a character string to distinguish this checkpoint from existing ones.
Keep	Enter the number of days and select the number of hours for which the checkpoint is to be retained. This information is displayed each time a user rolls the mouse over the checkpoint in the Schedule Checkpoints panel.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Segment Properties Window

This window enables you to view the properties of a selected segment. You can open this window by right-clicking a segment from System Manager and selecting Properties.

The following table describes the fields and buttons on this panel.

TABLE F-26 Fields and Elements on the Attach Segments Panel

Field	Description
Name	The name of the segment.
LUN	The logical unit number (LUN) on which the segment exists.
Size	The size of the segment.

TABLE F-26 Fields and Elements on the Attach Segments Panel (*Continued*)

Field	Description
Partition	The partition associated with the selected segment.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

View Volume Partitions Panel

This panel enables you to view the logical unit numbers (LUNs) available to the system and the volumes that are associated with the LUNs.

The following table describes the fields and buttons on this panel.

TABLE F-27 Fields and Elements on the View Volume Partitions Panel

Field	Description
Volumes	Click the volume to view its location on the existing LUNs.
Legend	Indicators in the graphical depiction of the LUN configuration: <ul style="list-style-type: none"> • Orange - Indicates the primary partition on the LUN. • Light Blue - Indicates the segmented partition on the LUN. • Green - Indicates the file-volume mirror (applicable only with the Sun StorageTek File Replicator option is licensed and enabled). • Blue - Indicates the DOS read-only attribute is applied to the LUN. This DOS read-only attribute is only used on the flash disk for the system volume. • White - Indicates the free space on the LUN. • Brown - Indicates the raw partition on the LUN, if any. The selected volume on a LUN is indicated by diagonal lines (///).
LUN	The name of the LUN on which the selected volume resides.
Partition #	The LUN partition on which the volume resides.
Use (%)	The percentage of space used on the volume.
Type	The type of volume, such as primary, segmented, or raw.
Free (MB)	The amount of space available for storage use in megabytes.
Capacity (MB)	The total amount of space for storage use in megabytes.

High Availability Panels

This section describes the fields and elements on the High Availability panels:

- [“Enable Failover Panel” on page 378](#)
- [“Recover Panel” on page 379](#)
- [“Set LUN Path Panel” on page 380](#)
- [“Set Primary Path Window” on page 381](#)

Enable Failover Panel

Note: This panel is available only for cluster configurations (appliances and gateway systems).

Use this panel to enable head failover for your cluster appliance or gateway system. A failover occurs when one of the servers (heads) in a dual-server system fails. The functioning server takes over or manages the Internet Protocol (IP) addresses and logical unit numbers (LUNs) formerly managed by the failed server. When the failed server is manually brought back online, original ownership or control of the said LUNs and IP address is restored in a process called failback or recovery. For more information about failover, see [“About Enabling Failover” on page 21](#).

Note: When a failed server is brought back online, you must initiate the recovery process from the Recover panel. For more information, see [“Initiating Recovery” on page 24](#).

The following table describes the fields and buttons on this panel.

TABLE F-28 Fields and Elements on the Enable Failover Panel

Field	Description
Automatic Failover	Click to have the system initiate failover in the event of a server failure.
Head Status	An indicator of the health of the server.
<i>Link Failover</i>	

TABLE F-28 Fields and Elements on the Enable Failover Panel (Continued)

Field	Description
Enable Link Failover	Click to enable link failover, which ensures that head failover occurs when any network interface that is assigned a “primary” role fails. This type of failure is referred to as a “link down” condition. If the partner’s network link is down, the server that wants to induce the failover must wait the specified amount of time after the partner server reestablishes its network link. Note: The system must be rebooted after enabling or disabling link failover for the change to take effect.
Down Timeout	The number of seconds a server waits before inducing head failover, in the event that the network link on one server becomes unreliable and the network link on its partner server is healthy.
Restore Timeout	The number of seconds the partner server’s primary link must be up in order for the failover to take place. The Restore Timeout is used only when a link down induced failover is initiated but aborted due to the partner server’s primary link being down.
<i>Partner Configuration</i>	
Name	The name of the partner server.
Gateway	The gateway IP address of the partner server.
Private IP	The IP address reserved for the heartbeat connection between the two servers. The IP address cannot be changed.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Recover Panel

Note: This panel is available only for cluster configurations (appliances and gateway systems).

This panel enables you to initiate recovery after a failed server (head) is brought back online. You must verify that the failed server is operable and online before proceeding to the recovery process.

You can also transfer LUN ownership to another server using the Recover panel. For example, if you create a LUN on head 1, you can select the LUN from the (NEW) Restore RAID Configuration list, click >, and click Apply to transfer ownership to head 2. You can only transfer LUN ownership to the other server in the cluster, you cannot take ownership of the other server’s LUNs.

The following table describes the fields and buttons on this panel.

TABLE F-29 Fields and Elements on the Recover Panel

Field	Description
<i>Current RAID Configuration</i>	
Head 1	The name of the server, designated as Head 1, that you want to recover.
Head 2	The name of the server, designated as Head 2, that you want to recover.
<i>(NEW) Restore RAID Configuration</i>	
Controller 0/Head 1	Depending on your configuration, this is either the logical unit number (LUN) mapping for controller 0 or the LUN mapping for Head 1.
Controller 1/Head 2	Depending on your configuration, this is either the LUN mapping for controller 1 or the LUN mapping for Head 2.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.
Apply	Click to save your changes.
Recover	Click to Recover the selected server.

Set LUN Path Panel

This panel enables you to define, edit, and restore, the logical unit number (LUN) paths for a file volume.

A LUN path is a designation of the hardware route, from server to redundant array of independent disks (RAID) controller, used to access a file volume in a LUN. Every file volume has two LUN paths. The alternate path is used when the primary path fails.

The following table describes the fields and buttons on this panel.

TABLE F-30 Fields and Elements on the Set LUN Path Panel

Field	Description
LUN	The LUN on which file volumes are located.
Volumes	The specific file volumes on the LUN.

TABLE F-30 Fields and Elements on the Set LUN Path Panel *(Continued)*

Field	Description
Active Path (HBA/SID)	The currently active hardware path over which the LUN communicates with the system. Hardware paths are identified by the host bus adapter (HBA) number, starting with 1, and the Small Computer Systems Interface (SCSI) identifier (ID) number of the first drive in the LUN, which is the controller. For example, 1/1 designates HBA 1 and SCSI controller target 1.
Primary Path (HBA/SID)	The preferred hardware path over which the LUN communicates with the system. The primary path is also the path to which a LUN path can be “restored.” If a primary path is not specified, the system uses the first available path.
Alternate Path (HBA/SID)	The alternate hardware path over which the LUN can communicate with the system if the primary path fails.
Edit	Click to launch the Primary Path window. From this window, you can edit the primary path for the selected volumes.
Restore	Click to restore the active path to the primary path for the selected volumes.
Auto-assign LUN Paths	Click to have the software assign LUN paths to the selected volumes.

Set Primary Path Window

This window enables you to define the primary path, which is the hardware route that the software uses to send information to the shared logical unit number (LUN). The secondary path is used when the primary path fails.

The following table describes the fields and buttons on this panel.

TABLE F-31 Fields and Elements on the Set Primary Path Window

Field	Description
LUN Name	The read-only name of the LUN for which you are setting the primary path.
Primary Path	The host bus adapter (HBA) and Small Computer Systems Interface (SCSI) identifier (ID) that define the path. Select the path you want from the drop-down menu.
Volumes	The read-only name of the volume on the selected LUN.

TABLE F-31 Fields and Elements on the Set Primary Path Window (*Continued*)

Field	Description
Text box	A line of text that indicates the HBAs, SIDs, and the status of the available paths.
Apply	Click to save your changes.
Cancel	Click to clear the fields of any entries and close out of the window without saving the changes.

iSCSI Configuration Panels

This section describes the fields and elements on the iSCSI Configuration panels:

- [“Add/Edit iSCSI Access Window” on page 382](#)
- [“Add/Edit iSCSI LUN Window” on page 383](#)
- [“Configure Access List Panel” on page 385](#)
- [“Configure iSCSI LUN Panel” on page 385](#)
- [“Configure iSNS Server Panel” on page 386](#)
- [“Promote iSCSI LUN Window” on page 386](#)

Add/Edit iSCSI Access Window



This window enables you to create or edit an Internet Small Computer Systems Interface (iSCSI) access list, depending on whether you accessed the window by clicking Add or Edit. An iSCSI access list defines a set of iSCSI initiators that can access one or more iSCSI logical unit numbers (LUNs) on the NAS device. When you define each iSCSI LUN, you will associate the appropriate access list with that LUN.

The following table describes the fields and buttons in this window.

TABLE F-32 Fields and Elements on the Add/Edit iSCSI Access Window

Field	Description
Name	The name of the access list, specified as any one or more characters.

TABLE F-32 Fields and Elements on the Add/Edit iSCSI Access Window (*Continued*)

Field	Description
CHAP Initiator Name	The full name of the Challenge Handshake Authentication Protocol (CHAP) initiator that is configured by the iSCSI initiator software. The default CHAP initiator name for a Windows iSCSI client is: <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	The CHAP initiator password (minimum of 12 characters).
Initiator IQN Name	The initiator iSCSI Qualified Name (IQN) name, specified as any one or more characters. If you leave this field blank, any initiator can access the target.
	Click to add the Initiator IQN name to the list of initiators that can access the target LUN.
Initiator IQN List	The list of initiators that can access the target LUN.
	This button is available only if the target LUN that is associated with the selected initiator is inactive. Click to remove the selected initiator from the list. The initiator then no longer has access to the LUN.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit iSCSI LUN Window

This window enables you to add or edit an Internet Small Computer Systems Interface (iSCSI) logical unit number (LUN), depending on whether you accessed the window by clicking Add or Edit. An iSCSI LUN can be accessed by iSCSI initiators.

Before adding or editing an iSCSI LUN, ensure that you have created an access list for the LUN. For more information, see [“Creating an iSCSI Access List” on page 62](#).

The following table describes the fields and buttons in this window.

TABLE F-33 Fields and Elements on the Add/Edit iSCSI LUN Window

Field	Description
Name	<p>The name of the iSCSI LUN. The name can include one or more alphanumeric characters (a-z, A-Z, 0-9), hyphens (-) and periods (.), and colons (:).</p> <p>The target name you specify will be prefixed with the full iSCSI Qualified Name (IQN) name according to the following naming convention: <code>iqn.1986-03.com.sun:01:mac-address.timestamp.user-specified-name</code></p> <p>For example, if you type the name <code>lun1</code>, the full name of the iSCSI target LUN is: <code>iqn.1986-03.com.sun:01:mac-address.timestamp.lun1</code></p> <p>Note: The timestamp is a hexadecimal number representing the number of seconds after 1/1/1970.</p>
Alias	(Optional) A brief description about the target LUN.
Volume	The name of the NAS file volume where the iSCSI LUN will be created.
Capacity	The maximum size for the LUN, in bytes, kilobytes, megabytes, or gigabytes (maximum of 2 terabytes).
Thin Provisioned	<p>Select the Yes checkbox to create a thin provisioned LUN. A thin provisioned LUN sets the file size attribute to the specified capacity, but the disk blocks are not allocated until data is written to the disk.</p> <p>If you create a non-thin provisioned LUN, disk blocks will be allocated based on the capacity of the LUN you are creating. When creating non-thin provisioned iSCSI LUNs, allow approximately 10% extra space on the volume for file-system metadata. For example, a 100 gigabyte iSCSI LUN must reside on a 110 gigabyte volume to allow non-thin provisioned LUN creation.</p> <p>For more information about deciding to use thin provisioned or non-thin provisioned LUNs, see “About SCSI Thin-Provisioned LUNs” on page 63.</p>
Access	Select the existing access list for this LUN from the drop-down list.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Configure Access List Panel

This panel displays the access lists defined for the NAS OS. An Internet Small Computer Systems Interface (iSCSI) access list defines a set of iSCSI initiators that can access one or more iSCSI logical unit numbers (LUNs) on the NAS device.

From this panel, you can add, remove, or edit an access lists.

The following table describes the fields and buttons on this panel.

TABLE F-34 Fields and Elements on the Configure Access List Panel

Field	Description
Name	Name of the access list.
CHAP Initiator Name	Name of the Challenge Handshake Authentication Protocol (CHAP) initiator that is configured by the iSCSI initiator software.
Add	Click to launch the Add iSCSI Access window. From this window, you can add a new access list.
Remove	Click to remove the selected access list from the Configure Access List table.
Edit	Click to launch the Edit iSCSI Access window. From this window, you can edit the selected access list.

Configure iSCSI LUN Panel

This panel displays the Internet Small Computer Systems Interface (iSCSI) logical unit numbers (LUNs) defined to the NAS OS.

From this panel, you can add, remove, or edit iSCSI LUN definitions. You can also promote an iSCSI LUN (applicable after promoting the corresponding file volume).

The following table describes the fields and buttons on this panel.

TABLE F-35 Fields and Elements on the Configure iSCSI LUN Panel

Field	Description
Name	The name of the iSCSI LUN.

TABLE F-35 Fields and Elements on the Configure iSCSI LUN Panel (*Continued*)

Field	Description
Alias	A brief description about the target LUN.
Volume	The name of the volume on which the iSCSI LUN is to be created.
Promote iSCSI LUN	Click to launch the Promote iSCSI LUN window.
New	Click to launch the Add iSCSI LUN window. From this window, you can add a new iSCSI LUN.
Remove	Click to remove the selected iSCSI LUN from the Configure Access List table.
Edit	Click to launch the Edit iSCSI LUN window. From this window, you can edit the selected iSCSI LUN.

Configure iSNS Server Panel

Use this panel to enable use of an Internet Storage Name Service (iSNS) server for iSCSI target discovery. The NAS iSNS client inter-operates with any standard iSNS server, such as Microsoft iSNS Server 3.0.

The following table describes the fields and buttons on this panel.

TABLE F-36 Fields and Elements on the Configure iSNS Server Panel

Field	Description
iSNS Server	The Internet Protocol (IP) address or Domain Name Service (DNS) name of the iSNS server.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Promote iSCSI LUN Window

After promoting a file volume that contains iSCSI logical unit numbers (LUNs), you must promote each iSCSI LUN on that file volume. This panel enables you to promote an iSCSI LUN.

The following table describes the fields and buttons on this panel.

TABLE F-37 Fields and Elements on the Promote iSCSI LUN Panel

Field	Description
Name	iSCSI target IQN identifier for the LUN to be promoted (as displayed on the Configure iSCSI LUN panel).
Alias	A brief description about the LUN. This field is filled in based on the original iSCSI LUN definition, but you can change it, if desired.
Volume	The name of the file volume name of the file volume where the promoted LUN resides (that is, the name of the file volume as it was just promoted).
Access	The name of the access list
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Monitoring and Notification Panels

This section describes the fields and elements on the Monitoring and Notification panels:

- [“Configure SNMP Panel” on page 388](#)
- [“Configure System Auditing Panel” on page 388](#)
- [“Diagnostic Email Window” on page 389](#)
- [“Display System Log Panel” on page 390](#)
- [“Set Up Email Notification Panel” on page 391](#)
- [“Set Up Logging Panel” on page 392](#)
- [“Set Up UPS Monitoring Panel” on page 394](#)
- [“View Fan Status Panel” on page 394](#)
- [“View File Volume Usage Panel” on page 395](#)
- [“View Power Supply Status Panel” on page 396](#)
- [“View Temperature Status Panel” on page 397](#)
- [“View Voltage Regulator Status Panel” on page 397](#)

Configure SNMP Panel

This panel enables you to configure Simple Network Management Protocol (SNMP) monitoring. SNMP is an industry standard for coordinating the operation of diverse network devices.

The following table describes the fields and buttons on this panel.

TABLE F-38 Fields and Elements on the Configure SNMP Panel

Field	Description
Enable SNMP	Click to enable SNMP monitoring for the system.
Server SNMP Community Name	The name of the SNMP community to which the system belongs.
Contact Info	The name of the person who is responsible for this system.
System Location	The network location of the system. This location can be physical or logical.
Destination IP Address	The Transmission Control Protocol/Internet Protocol (TCP/IP) address for the server that is designated as an SNMP trap destination, in the event of system errors.
Port #	The port to which the system will send traps. The default value is port 162.
Version	The SNMP protocol version (either 1 or 2).
Community	The community string for the trap destination.
Enable	Click to enable this target address to become a trap destination.
Remove	To remove a trap destination, select it and then click the Remove button.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure System Auditing Panel

This panel enables you to configure system auditing. You can set up system auditing so that records of particular system events are stored in separate audit log files.

Note: There is no Web Administrator graphical user interface support for reading or removal of audit logs. To read audit log files, you must use the `praudit` command, which converts the binary information in the audit logs into readable text.

The following table describes the fields and buttons on this panel.

TABLE F-39 Fields and Elements on the Configure System Auditing Panel

Field	Description
Enable System Auditing	Select to enable system auditing.
<i>Log File Configuration</i>	
Store Log Files to Volume	The volume on which system audit log files are stored. Note: Selectable volumes are non-system volumes. You must create special purpose audit volumes. (For instructions, see “Creating a File Volume or Segment Using the Create File Volumes Panel” on page 51.)
Max Log File Size (1 to 1024)	The largest size to which a system audit log file can grow, from 1 to 1024 megabytes.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Diagnostic Email Window



This window lets you send email notifications to recipients.

The following table describes the fields and buttons on this panel.

TABLE F-40 Fields and Elements on the Diagnostic Email Window

Field	Description
Problem Description	Type a description of the problem in this text field. This is a mandatory entry and is limited to 256 characters.
<i>Recipient Information</i>	
Email Address	Type the email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.

TABLE F-40 Fields and Elements on the Diagnostic Email Window (Continued)

Field	Description
<i>List</i>	
	Click to add the new recipient to the list of recipients.
	Click to remove the selected recipient from the list of recipients.
Recipient	The email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.
Send	Click to send the email notification.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.
Save Recipients List	Click to save the new recipient to the list.

Display System Log Panel

This panel enables you to selectively view, print, and save system log messages. The system software logs and displays the following types of events:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug

The following table describes the fields and buttons on this panel.

TABLE F-41 Fields and Elements on the Display System Log Panel

Field	Description
File	The name of the log file that you are viewing. This field is blank when you are viewing the system log file.

TABLE F-41 Fields and Elements on the Display System Log Panel *(Continued)*

Field	Description
Date	The date upon which the event occurred.
Time	The time, in military format, at which the event occurred.
Description	A line of text that describes the event.
Event Types	Click the types of events that you want displayed on this panel. To update the log file so that it displays only the selected event types, click Refresh.
Print	Click to print the log.
Save As	Click to save the log as an HTML file on your local system.
Silence Alarm	(Sun StorageTek 5210 NAS appliances only.) Click to silence the redundant array of independent disks (RAID) alarm.

Set Up Email Notification Panel

This panel enables you to set the name of the Simple Mail Transport Protocol (SMTP) server and designate email notification recipients. In the event of a system error, the system will send a detailed email message to the designated recipients through the SMTP server.

Recipient email addresses are displayed in the List box. When an error is detected, the system logs the error in the system log file and sends email notifications and warnings to the listed recipients.



Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-42 Fields and Elements on the Set Up Email Notification Panel

Field	Description
SMTP Server Name	The name of the SMTP server.
Mail From	The email address of the sender.
Email Address	The email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.

TABLE F-42 Fields and Elements on the Set Up Email Notification Panel (Continued)

Field	Description
<i>List</i>	
	Click to add the new recipient to the list of recipients.
	Click to remove the selected recipient from the list of recipients.
Recipient	The email address of the recipient.
Notification	Click to have notifications sent to the email recipient.
Diagnostics	Click to have diagnostic information sent to the email recipient.
<i>Notification Level</i>	
Errors	Select to notify recipients of system errors but not system warnings.
Errors and Warnings	Select to notify recipients of all system warnings and errors.
None	Select to disable email notifications. The appliance or gateway system will not send any notifications.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Logging Panel

This panel enables you to set up logging for the system. You can enable remote logging if your system includes a `syslogd` Unix server.

Before you can enable remote logging, the following conditions must be met:

- The system must be able to send the system log to this remote `syslogd` server. (See [“Setting Up Logging” on page 35.](#))
- DNS settings must be configured.

The following table describes the fields and buttons on this panel.

TABLE F-43 Fields and Elements on the Set Up Logging Panel

Field	Description
Enable Remote Syslogd	Click to enable the system message logger and its designated server.

TABLE F-43 Fields and Elements on the Set Up Logging Panel *(Continued)*

Field	Description
Server	The name of the server to which the system log will be sent.
Facility	From the drop-down menu, select the facility code to be assigned to all NAS messages that are sent to the log.
Facility	Select the types of system events for which to generate log messages. Each type of event represents a different priority, or severity level: <ul style="list-style-type: none">• Emergency – Specifies emergency messages. These messages are not distributed to all users. Emergency priority messages can be logged into a separate file for reviewing.• Alert – Specifies important messages that require immediate attention. These messages are distributed to all users.• Critical – Specifies critical messages not classified as errors, such as hardware problems. Crit 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.• Info – Specifies informational messages. These messages are useful in analyzing the system.• Debug – Specifies debugging messages.
Enable Local Log	Click to enable local system logging, which enables the system to save log messages locally.
Local File	The path and file name of the system log. The log cannot be written to the /cvol or /dvol directory.
Archives	The maximum number of archive files, from 1 to 9.
Size	The maximum allowable size, in kilobytes, for each archive file. The allowable range is from 100 through 999,999 kilobytes.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up UPS Monitoring Panel

This panel enables you to set up uninterruptible power supply (UPS) monitoring (not UPS management). For more information about the UPS events that can be monitored, see [“About UPS Monitoring” on page 168](#).

Note: Before you can enable UPS monitoring on this panel, the UPS monitoring service must be connected to the system. Otherwise, the UPS monitoring system will notify you that there is a UPS failure.

The following table describes the fields and buttons on this panel.

TABLE F-44 Fields and Elements on the Set Up UPS Monitoring Panel

Field	Description
Enable UPS Monitoring	Click to enable UPS monitoring for the system. In order to work properly, the UPS monitoring service must be connected to the system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

View Fan Status Panel

This panel enables you to view the status and revolutions per minute (RPMs) of each fan assembly in the appliance or gateway server.

The following table describes the fields and buttons on this panel.

TABLE F-45 Fields and Elements on the View Fan Status Panel

Field	Description
Fan	The fan for which you are viewing a status condition.

TABLE F-45 Fields and Elements on the View Fan Status Panel (*Continued*)

Field	Description
Status	A visual indicator of the status of the fan: <ul style="list-style-type: none"> • Green diamond - The RPMs are normal for this fan. • Red diamond - The RPMs have exceeded an acceptable range for this fan. If the revolutions per minute fall below 1800 for a fan, an email notification will be sent to the designated email recipients. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 34.
RPM	The number of RPMs for the fan.

The identification of fans vary, depending on where it is being viewed: from the Web Administrator interface, event log, or the physical label, as shown in [“Sun StorageTek 5320 NAS Appliance Server Fan Identification” on page 395](#).

TABLE 4-2 Sun StorageTek 5320 NAS Appliance Server Fan Identification

Web Administrator	Label on Fan	syslog/remote syslog
1	FT0/FM0	0
2	FT0/FM1	1
3	FT0/FM2	2
4	FT1/FM0	3
5	FT1/FM1	4
6	FT1/FM2	5

View File Volume Usage Panel

This panel enables you to view how each file volume is being used.

The following table describes the fields and buttons on this panel.

TABLE F-46 Fields and Elements on the View File Volume Usage Panel

Field	Description
Name	The name of the file volume.
Capacity	A graphical representation of the amount of space used on the file volume and the amount of space available to be used.

TABLE F-46 Fields and Elements on the View File Volume Usage Panel (*Continued*)

Field	Description
Volume Status	The status of the volume: read/write (r/w) or read only (r/o).
Requests	The number of requests processed for the volume since the volume was mounted.
Active	The number of requests processed for the volume in the last ten minutes.

View Power Supply Status Panel

This panel enables you to view the current status of all power supplies for the system.

The following table describes the fields and buttons on this panel.

TABLE F-47 Fields and Elements on the View Power Supply Status Panel

Field	Description
Power Supply	The power supply for which you are viewing a status condition.
Status	A visual indicator of the status of the power supply: <ul style="list-style-type: none">• Green diamond - The voltage and temperature levels are normal for this power supply.• Red diamond - The voltage and temperature levels have exceeded the acceptable range. An email will be sent to the designated email recipients to notify them of this condition. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 34.
Description	The status condition of the power supply. The status is one of the following: <ul style="list-style-type: none">• Green - Normal• Red - Failed or AC Missing• Red - AC power missing• Red - Power supply has failed• Red - The power supply is missing

View Temperature Status Panel

This panel enables you to view the temperature of the sensors in the appliance or gateway server.

The following table describes the fields and buttons on this panel.

TABLE F-48 Fields and Elements on the View Temperature Status Panel

Field	Description
Sensor	The sensor for which you are viewing a status condition.
Status	A visual indicator of the status of the sensor: <ul style="list-style-type: none">• Green diamond - The sensor is operating within the normal temperature range.• Red diamond - The temperature has exceeded the acceptable range. If the temperature rises above 55 degrees Celsius (131 degrees Fahrenheit), an email will be sent to the designated email recipients. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 34.
Value	The temperature of the sensor.

View Voltage Regulator Status Panel

This panel enables you to view the current readings for voltage regulators on the system. Voltage regulators are devices or circuits that regulate the voltage fed to a microprocessor.

The following table describes the fields and buttons on this panel.

TABLE F-49 Fields and Elements on the View Voltage Regulator Status Panel

Field	Description
Voltage Regulator	The voltage regulator for which you are viewing a status condition.

TABLE F-49 Fields and Elements on the View Voltage Regulator Status Panel (Continued)

Field	Description
Status	A visual indicator of the status of the power supply: <ul style="list-style-type: none">• Green diamond - The voltage level is normal for this voltage regulator.• Red diamond - The voltage level has exceeded the acceptable range for this voltage regulator. An email will be sent to the designated email recipients to notify them of this condition. For more information about setting up email notifications, see “Setting Up Email Notifications” on page 34.
Current Value	The number of volts currently being fed to the microprocessor.

Network Configuration Panels

This section describes the fields and elements on the Network Configuration panels:

- [“Bond NIC Ports Panel”](#) on page 398
- [“Configure Network Adapters Panel”](#) on page 400
- [“Create/Edit Port Bond Window”](#) on page 403
- [“Set Gateway Address Panel”](#) on page 404
- [“Set Server Name Panel”](#) on page 405
- [“Set Up DNS Panel”](#) on page 406
- [“View the Routing Table Panel”](#) on page 407

Bond NIC Ports Panel

This panel enables you to add, edit, remove, and recover network interface card (NIC) port bonds.

The following table describes the fields and buttons on this panel.

TABLE F-50 Fields and Elements on the Bond NIC Ports Panel

Field	Description
Bond ID	The unique NIC port bond designation for this bond.

TABLE F-50 Fields and Elements on the Bond NIC Ports Panel (Continued)

Field	Description
Type	<p>The type of bond, which can be either of the following:</p> <ul style="list-style-type: none">• Port aggregation – Also known as “channel bonding” or “trunking.” Lets you scale network I/O by joining NIC ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth. You must have a minimum of two available NIC ports for port bonding. Note: All NIC ports in an aggregation bond must be of the same type of interface card (such as, Fast Ethernet with Fast Ethernet), be connected to the same subnet, and be connected to adjacent ports. For systems that use switches, the switches must support port (or channel) bonding.• High availability – Provides NIC port failover. Multiple NIC ports can be bonded to a primary port as back-up ports. When the primary port fails, the software switches to the back-up port at the top of the list of high-availability bonded ports. If that port also fails, the port next on the list is used, and so on. Note: NICs in a high availability bond do not have to be the same type of interface card or be connected to the same subnet.
Status	<p>Color coded statuses:</p> <ul style="list-style-type: none">• Normal (green)• Failover (yellow)• Down (red) – This occurs if the ports fail, if the primary port and slave ports in a high-availability bond fail, or if failover is unsuccessful.
IP Address	The Internet Protocol (IP) address designated for the port bond.
Subnet Mask	The subnet mask associated with the bond.
Broadcast Address	The broadcast address associated with the bond.
Slaves	Any slave ports in the bond.
New	Click to launch the Create Port Bond window. From this window, you can create a new port bond.
Edit	Click to launch the Edit Port Bond window. From this window, you can edit the selected port bond.
Remove	Click to remove the port bond from the table.
Recover	Click to recover from a NIC port failover. Clicking Recover starts the recovery process. The failed NIC port must be online before you attempt to recover.

Configure Network Adapters Panel

This panel enables you to configure Dynamic Host Configuration Protocol (DHCP) for the system or specify the Internet Protocol (IP) address, netmask, and broadcast for each network controller. In addition, this panel enables you to add IP aliases for each network interface card (NIC).

The following table describes the fields and buttons on this panel.

TABLE F-51 Fields and Elements on the Configure Network Adapters Panel

Field	Description
Enable DHCP	Click to enable DHCP. DHCP enables the system to dynamically acquire an IP address from the DHCP server. If you want to manually configure the static IP address, subnet mask, and/or gateway IP, do not select this checkbox.
Adapter	A list of the existing NIC ports. If you have already created a port bond, that port bond is displayed in this list. Ports that are not bonded are labeled Port <i>x</i> , whereas ports that are bonded are labeled Bond <i>x</i> . Note: If ports are bonded, you cannot create alias IP addresses for each port, but instead you create the alias for the bond. For example, if you have bonded Port 2 and Port 3 to form Bond 1, you cannot add alias IP addresses to Port 2 or Port 3. You can only add aliases to Bond 1.
IP Address	The primary IP address for the NIC port that is selected in the Adapters list.
Netmask	An indicator that shows which portion of an IP address identifies the network address and which portion identifies the host address.
Broadcast	The read-only broadcast address for the NIC port that is selected in the Adapters list. The broadcast address is the IP address used to send broadcast messages to the subnet.

TABLE F-51 Fields and Elements on the Configure Network Adapters Panel (Continued)

Field	Description
Role	<p>The role for the NIC port that is selected in the Adapters list. Valid roles are as follows:</p> <ul style="list-style-type: none"><li data-bbox="605 302 1310 638">• Primary – This port role identifies an active network port. At least one port must be assigned a primary role. In cluster configurations, the primary port plays an integral part in the failover process. When you assign this role to a port, the partner server in the cluster saves a copy of the IP address of that port as an inactive alias IP address. In addition, when you configure alias IP address on either server, the partner server holds those IP address as additional inactive alias IP addresses. If a failover occurs, the healthy server activates the inactive alias IP addresses corresponding to the IP addresses for the failed server, allowing network access to continue as if the failed server were still active. You cannot aggregate primary NIC ports.<li data-bbox="605 696 1310 864">• Independent – This port role designates an active network port used for purposes other than serving data. Independent ports are typically used for remote backup. Identify at most one independent port per server. You cannot aggregate independent NIC ports or configure alias IP addresses for them.<li data-bbox="605 874 1310 1072">• Mirror – This port role is applicable only with the Sun StorageTek File Replicator option is licensed and enabled. It indicates that the port connects this server to another server for purposes of mirroring file volumes. Use the same port on both the source and target servers for mirroring. For more information about mirroring, see “About Mirroring” on page 133. Mirror ports support port aggregation and alias IP addressing.<li data-bbox="605 1083 1310 1248">• Private – This port role is applicable only for cluster appliances and cluster gateway systems. It is reserved for the heartbeat, a dedicated network link that constantly monitors the status of the other server. Each server in a dual-server configuration has one and only one private port. You cannot configure alias IP addresses for private ports.

TABLE F-51 Fields and Elements on the Configure Network Adapters Panel (Continued)



Field	Description
Interface	<p>Interface-specific information that applies to the selected NIC port:</p> <ul style="list-style-type: none">• Description – A line of text that describes the selected adapter.• H/W Address – The Hardware (H/W) or Media Access Control (MAC) address, which is a unique address in hexadecimal format, that is used by network software to distinguish this network card from others on the network. This address is encoded on the network card at the factory.• Speed – The speed (Mb data/sec) at which data is transmitted over the network.• MTU/Max MTU – The current Maximum Transmission Unit (MTU) of the selected adapter. MTU is the largest frame length that can be sent on a physical medium. The maximum MTU value is the default value of 1500. The minimum value is 552. The TCP Max segment size is the IP Maximum datagram size minus 40. The default IP Maximum Datagram Size is 576. The default TCP Maximum Segment Size is 536.
Statistics	<p>Input/Output (I/O) information about the selected NIC port:</p> <ul style="list-style-type: none">• Packets In/Out – The number of packets in and out for this NIC port.• Errors In/Out – The number of errors in and out for this NIC port.• Collisions – The number of transmission collisions for this NIC port.• Clear Counters – Click to clear all counts on the Statistics tab: packets, errors, and collisions.
IP Aliases	<p>The alias IP address applied to the selected NIC port. There can be up to nine aliases for single-server systems, and up to four aliases for dual-server systems. For dual-server systems only, the value in this field can be the primary IP address of the corresponding port on the partner server, if necessary.</p> <p>Typically, IP aliases specify the IP addresses of obsolete systems that have been replaced by NAS storage.</p>
Partner IP Aliases	<p>The primary IP address of the corresponding port on the partner server, if necessary. This field displays the IP addresses of the partner server that are reserved for back-up purposes. These are the IP addresses that will be activated by the remaining server in the event of a failover. This field is available only for dual-server systems.</p>
	<p>Click to move the IP alias value that you typed from the IP Aliases field into the list of available IP aliases.</p>
	<p>Click to remove the selected IP alias from the list of available IP aliases.</p>
Apply	<p>Click to save your changes.</p>

TABLE F-51 Fields and Elements on the Configure Network Adapters Panel *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Create/Edit Port Bond Window

This window enables you to create or edit a bond between two or more network interface card (NIC) ports. This bond forms either a port aggregation bond or a high availability bond.



In a port aggregation bond, ports are combined to produce a higher bandwidth port. All NICs in this type bond must be of the same type of interface card (for example, Fast Ethernet with Fast Ethernet) and connect to the same subnet. In a high availability bond, ports are bonded to create port failover (NIC port redundancy). In this type of bond, NICs can be of different type of interface cards and be connected to different subnets.

The following table describes the fields and buttons in this window.

TABLE F-52 Fields and Elements on the Create/Edit Port Bond Window

Field	Description
IP Address	The Internet Protocol (IP) address designated for the port bond.
Subnet Mask	This field is available only if DHCP is disabled. The subnet netmask for the first NIC port added to the port bond.
Broadcast Address	The broadcast address associated with the bond. This broadcast address is used by the first NIC port (the primary port) listed in the NIC Ports in This Bond field.
Partner IP Address	(Dual-server configuration only) Type the IP address of the partner server that will be activated by the remaining server in the event of a failover.

TABLE F-52 Fields and Elements on the Create/Edit Port Bond Window (*Continued*)

Field	Description
Port Aggregation	<p>The type of bond, also known as “channel bonding” or “trunking.” Lets you scale network I/O by joining NIC ports. This forms a single network channel of high bandwidth from two or more channels of lower bandwidth. You must have a minimum of two available NIC ports for port bonding.</p> <p>Note: All NIC ports in an aggregation bond must be of the same type of interface card (for example, Fast Ethernet with Fast Ethernet), be connected to the same subnet, and be connected to adjacent ports. For systems that use switches, the switch must support port (or channel) bonding.</p>
High Availability	<p>The type of port bond that provides NIC port failover. Multiple NIC ports can be bonded to a primary port as back-up ports. When the primary port fails, the software switches to the back-up port at the top of the list of high-availability bonded ports. If that port also fails, the port next on the list is used, and so on.</p> <p>Note: NICs in a high-availability bond do not have to be the same type of interface card or be connected to the same subnet.</p>
Available NIC Ports	<p>The NIC ports available to be bonded.</p> <p></p> <p>Click the top button to move the selected port from the Available NIC Ports box to the NIC Ports in This Bond box. Click the bottom button to move the selected port from the NIC Ports in This Bond box to the Available NIC Ports box.</p>
NIC Ports in This Bond	<p>The ports that already exist in this bond.</p> <p></p> <p>If this is a high availability bond type, use the up and down arrow buttons to organize the order of the ports. The first port in the NIC Ports in This Bond list is the primary port. The second port is the first port to be used in case of a failover. The next port in the list is used in case the port before it also fails.</p>
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Set Gateway Address Panel

This panel enables you to specify the gateway address.

The following table describes the fields and buttons on this panel.

TABLE F-53 Fields and Elements on the Set Gateway Address Panel

Field	Description
Gateway	The gateway address for the system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Server Name Panel

This panel enables you to configure basic information about the NAS server on your network.

The following table describes the fields and buttons on this panel.

TABLE F-54 Fields and Elements on the Set Server Name Panel

Field	Description
Server Name	The name by which the server is known on the network. The name must begin with a letter of the alphabet (a-z, A-Z) or number 0-9 and can include up to 30 alphanumeric characters: a-z, A-Z, 0-9, hyphens (-), underscores (_), and periods (.).
Company Name	The company name, up to 32 characters, that will be included in any diagnostic email messages sent from this system.
Contact Name	The contact name, up to 32 characters, that will be included in any diagnostic email messages sent from this system.
Contact Phone #	The phone number of the contact who will be included in any diagnostic email messages that are sent from this system.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up DNS Panel

This panel enables you to set up the Domain Name Service (DNS) name service, which includes specifying the domain name and adding or removing a DNS server.

Note: If you are using DNS without Dynamic DNS, you must add the host name and Internet Protocol (IP) address of the system to the DNS database before entering values on this panel. If you are using Dynamic DNS, you do not need to manually update the DNS database. For more information, see your DNS documentation.

Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-55 Fields and Elements on the Set Up DNS Panel





Field	Description
Enable DNS	Select to enable DNS on the system.
Domain Name	The DNS domain name, which is the name by which the domain is known to the network.
Server	The IP address of a DNS server that you want to make available to the network.
Server List	Each existing DNS server that is available to the network. The DNS server at the top of the list is queried first for domain name resolution.
	Click to add the server entry that you typed from the Server field to the Server List.
	Click to remove the selected server from the Server List.
	Click to move the selected server up one position in the Server List.
	Click to move the selected server down one position in the Server List.
Enable Dynamic DNS	Select to enable a dynamic DNS client to add the system into the DNS namespace. If you enable dynamic DNS, you must also configure the Kerberos realm and Key Distribution Center (KDC) server on the “Configure Domains and Workgroups Panel” on page 452. When Dynamic DNS is enabled, non-secure dynamic updates occur, if allowed by the DNS server.

TABLE F-55 Fields and Elements on the Set Up DNS Panel (Continued)

Field	Description
DynDNS User Name	The user name of a Windows 2000 user with whom the dynamic DNS client can authenticate to perform secure dynamic DNS updates. This user must reside within the Active Directory Service (ADS) domain and the Kerberos realm that is specified on the “Configure Domains and Workgroups Panel” on page 452. Note: If the domain administrator user name is displayed in this field but the ADS update fails, the domain administrator password must be changed (on the domain controller). This is only required for the administrator user, and the same password can be reused. For more information, see the Microsoft Support Services Web Site, Article Q248808.
DynDNS Password	The password of the DynDNS user. If you are updating this field, delete the entire password before entering a new one.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

View the Routing Table Panel

This panel enables you to view the following information about network routes.

TABLE F-56 Fields and Elements on the View the Routing Table Panel

Field	Description
Destination	The Internet Protocol (IP) address of the destination, which can refer either to a network or to a host. There must be one default route (such as, 0.0.0.0), one loop-back route (such as, 127.0.0.1), at least one network route, and at least one host route.
Gateway	The gateway address through which the packets travel to the destination.
Mask	The netmask for the destination network.
Interface	The type of interface that is used to send packets over the network.

TABLE F-56 Fields and Elements on the View the Routing Table Panel (*Continued*)

Field	Description
Flags	Indicators of the route status. Each type of status indication is represented by a combination of the following flags: u - route usable g - destination is a gateway h - host entry (net otherwise) r - host or net unreachable d - created dynamically (by redirect) m - modified dynamically (by redirect) D - message confirmed M - subnet mask present c - generate new routes on use x - external daemon resolves name l - generated by ARP or ISIS S - manually added 2 - protocol specific routing flag 1 - protocol specific routing flag

RAID Panels

This section describes the fields and elements on the RAID panels:

- [“Add Hot-Spare Window” on page 408](#)
- [“Add LUN Window” on page 409](#)
- [“Locate Drive Tray Window” on page 411](#)
- [“Locate Drive Window” on page 411](#)
- [“Manage RAID Panel” on page 412](#)
- [“View Controller/Enclosure Information Panel” on page 414](#)
- [“View LUN Information Panel” on page 415](#)

Add Hot-Spare Window

Use this window to designate a drive as a hot-spare for NAS appliances. You do so by clicking on the drive image that you want.

The following table describes the drive images and buttons in this window.

TABLE F-57 Drive Images and Buttons in the Add Hot-Spare Window

Drive	Indication
<i>Drive icons</i>	<p>Graphic representation of the drives in the NAS device. If you are using unassigned drives, select three or more drives for the new LUN. The icons reflect the status of each drive, as follows:</p> <ul style="list-style-type: none"> • For Sun StorageTek 5320 controller units and expansion units, see TABLE F-2 for a description of the drive-status icons. • For Sun StorageTek 5300 controller enclosures and expansion enclosures, see TABLE F-3 for a description of the drive-status icons. • For Sun StorageTek 5210 devices, see “Add LUN Window” on page 409.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Add LUN Window

Use this window to add a logical unit number (LUN) to the system configuration for Sun StorageTek 5210 NAS appliances.

To add a new LUN, first select (click on) each drive that will belong to the LUN. Select a minimum of three drives.

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

TABLE F-58 Sun StorageTek 5210 Add LUN Drive Status Indicators









Drive	Indication
<i>Controller enclosure drives</i>	
	Drive is available for LUN membership.
	Drive is selected for LUN membership.
	Drive is not available for LUN membership.
	Drive slot is empty (no drive present).

TABLE F-58 Sun StorageTek 5210 Add LUN Drive Status Indicators (*Continued*)

Drive	Indication
<i>Expansion enclosure drives</i>	
	Drive is available for LUN membership.
	Drive is selected for LUN membership.
	Drive is not available for LUN membership.
	Drive slot is empty (no drive present).

The following table describes the other fields and buttons in this window.

TABLE F-59 Fields and Buttons on the Add LUN Window



Field	Description
<i>New LUN Assignments</i>	
RAID Level	Redundant array of independent disks (RAID) configuration for the LUN (always RAID 5).
Controller	Number to identify the controller that will manage the new LUN.
Head ID	Applicable with dual-server systems. Unique identifier assigned to this server that will manage the LUN.
Create New File Volume	Select to create the new LUN on the physical drives selected, and to create a new file system on that LUN. Specify the name of the new file volume to the right.
Grow Existing Volume	Select to create a LUN on the physical drives selected, and to use that LUN to expand the storage for an existing file system. Select the target file system from the drop-down menu.
None	Select to create the new LUN, but to not create a file system on the LUN.
Apply	Click to save your changes.
Cancel	Click to cancel the request and clear all fields.

Locate Drive Window

Use this window to activate the drive indicator lights for one or more drives. This allows you to physically locate those drives.

The following table describes the drive images and buttons in the window.

TABLE F-60 Fields and Buttons on the Locate Drive Window



Field	Indication
<i>Drive Icons</i>	Graphic representation of the drives in each controller unit and each expansion unit. Select (click on) the drive you want to locate.: The icons reflect the status of each drive, as follows: <ul style="list-style-type: none">• For Sun StorageTek 5320 controller units and expansion units, see TABLE F-2 for a description of the drive-status icons.• For Sun StorageTek 5300 controller enclosures and expansion enclosures, see TABLE F-3 for a description of the drive-status icons.• For Sun StorageTek 5210 devices, see “Add LUN Window” on page 409
	Click to cause the drive indicator light or lights on the selected drive to flash.
	Click after physically locating the drive, to stop flashing the indicator lights.
Cancel	Click to close the window.

Locate Drive Tray Window

Use this window to activate the drive indicator lights for all drives in a specific controller unit or expansion unit. This allows you to physically locate the unit.

The following table describes the drive images and buttons in the window.

TABLE F-61 Fields and Buttons on the Locate Drive Tray Window

Field	Indication
<i>Drive Icons</i>	Graphic representation of the drives in each controller unit and expansion unit. Select (click on) any drive in the controller or expansion unit you want to locate. The icons reflect the status of each drive, as follows: <ul style="list-style-type: none">• For Sun StorageTek 5320 controller units and expansion units, see TABLE F-2 for a description of the drive-status icons.• For Sun StorageTek 5300 controller enclosures and expansion enclosures, see TABLE F-3 for a description of the drive-status icons.• For Sun StorageTek 5210 devices, see “Add LUN Window” on page 409
	Click to cause all drive indicator lights on the selected drive tray to flash.
	Click after physically locating the drive tray, to stop the flashing the indicator lights.
Cancel	Click to close the window.

Manage RAID Panel

This panel enables you to manage your redundant array of independent disks (RAID) array. The top portion shows a graphical representation of disks. The bottom portion lists logical unit number (LUN) information in tabular form.

Note: As an alternative navigational method on this panel, you can use your keyboard:

- To move to the next field or element on the panel, press the **Tab** key.
- To perform a function, such as launching a window, press the **Alt** key + Underlined character on a button. For example, to launch the New LUN window, press **Alt + a**.

The following table describes the fields and buttons on this panel.

TABLE F-62 Fields and Elements on the Manage RAID Panel

Field	Description
Legend	<p>A key that describes the status of the disks and the LUNs. LUNs do not use the black or pink status.</p> <ul style="list-style-type: none"> • Black - A disk is not present in the slot. (Does not apply to LUNs.) • Green - A disk is present in the slot and is functional (online). The disk does not need to be assigned to a LUN. • Orange - A LUN is rebuilding. The LUN Status field shows percent complete during the rebuilding process. After the LUN is rebuilt with a hotspare, the copy back process begins. The Status field shows percent complete during the copy back process. • Yellow - A LUN is being created as indicated on the disk and in the LUN Status field. • Red - A disk has failed. You can safely remove the disk for replacement. If the failed disk is not assigned to a LUN, the Status field changes to green (online) because rebuilding is not required. The LUN status field is red. • Pink - A disk has been replaced. (Does not apply to LUNs.)
LUN/Drive	The name of the drive.
Capacity	The total amount of space available for storage use on the selected LUN.
Status	The status of the drive in the LUN.
RAID Level	The RAID configuration.
LUN Ownership	The user who owns the LUN.
Remove LUN	Click to remove the selected LUN from the RAID array.
New LUN	Click to launch the Add LUN wizard and add a LUN to the RAID array. This button is available only if at least three drives are available in the RAID array.
Remove HS	Click to remove a hot-spare from the RAID array.
Rebuild	(Sun StorageTek 5210 NAS appliance only) Click to rebuild the LUN after replacing a failed disk.
Add HS	Click to launch the Add Hot-Spare window. From this window, you can add a hot-spare to the RAID array.
Locate Drive	Click to open the Locate Drive window, which is used to cause the drive indicator lights on a physical drive to flash.
Locate Drive Tray	Click to open the Locate Drive Tray window, which is used to cause the drive indicator lights to flash on all the physical drives in a specific controller unit or expansion unit.

View Controller/Enclosure Information Panel

This panel displays information about redundant array of independent disks (RAID) controllers and controller units.

The following table describes the fields and buttons on this panel.

TABLE F-63 Fields and Elements on the View Controller/Enclosure Information Panel

Field	Description
Controller Information	List of controllers for the NAS device.
Vendor	Name of the controller vendor.
Model	Model number of the controller.
Firmware Release	Release level of the controller firmware.
<i>Enclosure Information</i>	
Tray IDs or Enclosure identifiers	For Sun StorageTek 5310 and Sun StorageTek 5320 NAS appliances, the tray ID for the controller unit that houses the selected controller (top), as well as the tray ID for each expansion unit that is connected to the controller unit. For Sun StorageTek 5210 NAS appliances, a list of expansion enclosures.
Vendor	The name of the vendor for the controller unit or expansion unit.
Model	The model number of the controller unit or expansion unit.
Firmware Release	Applicable for Sun StorageTek 5310 and Sun StorageTek 5320 expansion units only. The release level of the expansion-unit firmware.

View LUN Information Panel

This panel enables you to view the logical unit numbers (LUNs) in the system.

The following table describes the fields and buttons on this panel.

TABLE F-64 Fields and Elements on the View LUN Information Panel

Field	Description
LUNs	A list of the LUNs in your system.
Vendor	The name of the LUN vendor.
Product	The LUN product.
Product Revision	The revision of the LUN product.
Size	The size of the LUN.
ID Type	The type of identifier used by the LUN.
Vendor ID	The identifier of the LUN vendor.
Vendor Specific ID	The identifier specific to the vendor.
Vendor Specific ID Extension	The extension of the identifier that is specific to the vendor.

System Activity Panels

This section describes the fields and elements on the System Activity panels:

- [“View Networking Activity Panel” on page 415](#)
- [“View System Activity Panel” on page 416](#)

View Networking Activity Panel

This panel enables you to view the number of I/O requests per second, for clients accessing the NAS appliance or gateway system.

The following table describes the fields and buttons on this panel.

TABLE F-65 Fields and Elements on the View Networking Activity Panel

Field	Description
Clients	The Internet Protocol (IP) address of the client.
Requests (IO/sec)	The number of I/O requests, per second.

View System Activity Panel

This panel enables you to view the I/O requests per second between the system and the peripheral devices with which it communicates. The following are the peripheral devices that can be displayed on this panel:

- CPU – System central processing unit (CPU)
- Memory – System random access memory (RAM)
- Port Aggregation x – Port aggregation x
- Controller x – Redundant array of independent disks (RAID) controller x
- dac1d0xx – Logical unit numbers (LUNs) xx
- PORTx – Network interface card (NIC) port x
- Host Adapter x – Internet Small Computer Systems Interface (iSCSI) host adapter x (for tape backup device)

Note: The names and number of devices being monitored will vary, depending on the appliance or gateway-system hardware configuration.

The following table describes the fields and buttons on this panel.

TABLE F-66 Fields and Elements on the View System Activity Panel

Field	Description
Device	The peripheral device that communicates with the system.
Current Load (IO/sec)	The current load of the device, in terms of I/O requests per second.
Peak Load (IO/sec)	The peak load (highest value) reached by the device, in terms of I/O requests per second.

System Backup Panels

This section describes the fields and elements in the System Backup panel.

Set Up NDMP Panel

This panel enables you to set up the architecture for the Network Data Management Protocol (NDMP), which is an open protocol for network-based backup. NDMP architecture lets you use any NDMP-compliant backup administration application to back up your network attached storage device.

You must configure the backup administration application to log into the systems and to locate the devices on which the file volumes reside. You must also configure the volumes to enable checkpoints and backup checkpoints.

See [“Setting Up NDMP Backups” on page 186](#) and [“Enabling File-System Checkpoints” on page 177](#).

The following table describes the fields and buttons on this panel.

TABLE F-67 Fields and Elements on the Set Up NDMP Panel

Field	Description
NDMP NIC	List of network interface card (NIC) adapters and port bonds that are configured with an independent or primary role. The following information displays for each: <ul style="list-style-type: none">• Adapter - Name of the NDMP NIC adapter or port bond.• IP Address - The IP address of the adapter or port bond. Select the port adapter or bond port used to transfer data to the backup tape drive (typically an interface configured with independent roles). Make sure the port you select connects to the gateway that is identified below this field.
Gateway	Display-only. IP address of the gateway through which clients from other subnets connect with the NDMP server. The selected NIC must be on the same subnet as the gateway in order to communicate with NDMP clients that are behind the gateway.
NDMP Log	Full path, such as <code>/vol_ndmp</code> , for the directory used to store intermediate backup data and a permanent log of backup history. The directory must be independent from the volumes scheduled for backup, and at least 2 gigabytes in size.
Apply	Click to save your changes.

TABLE F-67 Fields and Elements on the Set Up NDMP Panel (Continued)

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

System Manager Panels

This section describes the fields and elements in the System Manager panels:

- [“Edit NFS Export Window” on page 418](#)
- [“Server Properties Window” on page 419](#)
- [“Volume Properties Window” on page 419](#)

Edit NFS Export Window

This window enables you to update the access permission for the selected NFS export and update the mapping of the UID for root users.

The following table describes the fields and buttons in this window.

TABLE F-68 Fields and Elements on the Edit NFS Export Window

Field	Description
Hosts	The hosts to which the selected export is defined.
<i>Access</i>	
Read/Write	Select to assign read/write access privileges to the export.
Read/Only	Select to assign read/only access privileges to the export.
No Access	Select to assign no access privileges to the export.
<i>Map Root User</i>	
Anonymous User	Select to map the user ID (UID) of root users (users with a UID of 0) to the user ID of the anonymous user (the user <code>nobody</code>).
Root User	Select to have root users use the UID of root (<code>uid=0</code>).
Map to UID	Select to map the UID of root users to the UID that you specify in the field.
Apply	Click to save your changes.

TABLE F-68 Fields and Elements on the Edit NFS Export Window (Continued)

Field	Description
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Server Properties Window

This window enables you to view the basic properties of the appliance or gateway-system server. To open this window, right-click the volume name under System Manager.

The following table describes the fields and buttons in this window.

TABLE F-69 Fields and Elements on the Server Properties Window

Field	Description
Name	The name of the server.
Model	The model number of the server.
Serial #	The serial number of the server.
OS Version	The current version of NAS software running on the server.
Cancel	Click to close out of the window.

Volume Properties Window

This window enables you to view the properties of the selected volume. To open this window, right-click System Manager and select Properties.

The following table describes the fields and buttons on this window.

TABLE F-70 Fields and Elements on the Volume Properties Window

Field	Description
Label	The label of the volume.
Compliance	Whether compliance archiving software is enabled for the volume.

TABLE F-70 Fields and Elements on the Volume Properties Window (*Continued*)

Field	Description
Checkpoints	Whether checkpoints are enabled for the volume.
Quotas	Whether quotas are enabled for the volume.
Capacity	The total amount of storage space on the volume. A graphical representation of storage usage is displayed: <ul style="list-style-type: none">• Used – The amount of space used on the volume.• Free – The amount of space available for storage use on the volume.
<i>Partitions</i>	
Legend	Indicators in the graphical depiction of the selected logical unit number (LUN) configuration: <ul style="list-style-type: none">• Orange – Indicates the primary partition on the volume.• Light Blue – Indicates the segmented partition on the volume.• Green – Indicates the file-volume mirror (applicable only with the Sun StorageTek File Replicator option is licensed and enabled).• Blue – Indicates that the DOS read-only attribute is applied to the volume. This DOS read-only attribute is only used on the flash disk for the system volume.• White – Indicates the free space on the volume.• Brown - Indicates the raw partition on the LUN, if any.
Lun	The name of the LUN on which the selected volume resides.
Partition	The LUN partition on which the volume resides.
Use (%)	The percentage of space used on the volume.
Type	The type of volume, such as primary or segmented.
Free (MB)	The amount of space available on the volume for storage use, in megabytes.
Capacity (MB)	The total amount of space on the volume for storage use, in megabytes.
Cancel	Click to close out of the window.

System Operations Panels

This section describes the fields and elements on the System Operations panels:

- [“Online System Registration” on page 421](#)
- [“Activate Options Panel” on page 422](#)
- [“Add License Window” on page 423](#)

- “Assign Language Panel” on page 424
- “Enable Temporary Licenses Window” on page 424
- “Import Licenses Window” on page 425
- “Set Administrator Password Panel” on page 425
- “Set Remote Access Panel” on page 426
- “Set Time and Date Panel” on page 427
- “Set Up Time Synchronization Panel” on page 428
- “Shut Down the Server Panel” on page 430
- “Update Software Panel” on page 431

Online System Registration

This panel enables you to register your Sun account and NAS server information with Sun Services.

The following table describes the fields and elements in the Online System Registration panel:

TABLE F-71 Fields and Elements on the Online System Registration Panel

Field	Description
Disclaimer	Read the Sun privacy statement and click Agree to continue with the registration process.
Agree	Click the checkbox after reading and agreeing to the disclaimer.
If you do not have your Sun Account, click here to get it.	Click the link to go to the Sun Online Account Registration portal. Click Register to sign up for a Sun account.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.
<i>Sun Account</i>	
Sun Account ID	Enter the account ID supplied by Sun. If you do not have your account ID and password, click the link
Sun Account Password	Enter the account ID supplied by Sun.
May Sun Contact you	Click the checkbox to allow contact.

TABLE F-71 Fields and Elements on the Online System Registration Panel (*Continued*)

Field	Description
<i>Proxy Server</i>	
Http Proxy Server	If your site is using a proxy server to communicate with Sun, enter the name or IP address of the proxy server. Ask your network administrator for the names and port numbers of the proxy server.
Port	Enter the port number for the proxy server.
Proxy User Name	If your proxy server requires authentication, enter the proxy user name.
Proxy Password	Enter the proxy user name password.
<i>Options</i>	
Send Heartbeat Data?	Click the checkbox to allow data to be sent to Sun Services.
Send Fault Events?	Click the checkbox to allow data to be sent to Sun Services.

Activate Options Panel

This panel enables you to view existing licenses on the system, add licenses to and remove licenses from the system, and enable temporary licenses on the system.

The following table describes the fields and buttons on this panel.

TABLE F-72 Fields and Elements on the Activate Options Panel

Field	Description
Module	The name of the licensable module.
State	Whether the license is valid.
Status	Whether the license is active.
Origination	The date on which the license became active, in YYYYMMDD format. If this field displays a value of 00000000, the license is immediately active. Note: This date is validated against the secure clock.
Expiration	The date on which the license expires, in YYYYMMDD format. If this field displays the value of 00000000, the license never expires. Note: This date is validated against the secure clock.
Key	The unique license key assigned to the license.

TABLE F-72 Fields and Elements on the Activate Options Panel (Continued)

Field	Description
Add	<p>Click to launch the Add License window. From this window, you can add a new license to the appliance or gateway-system server.</p> <p>Note: Licenses cannot be added to the system until the secure clock is initialized. The secure clock is initialized the first time you set the date and time on the system. For more information, see “Setting the Time and Date Manually” on page 70.</p> <p>Make sure you set the time accurately, as the secure clock can only be set once. After you set the initial time and date, the license is not affected by additional changes to the time and date.</p>
Remove	Click to delete the selected license from the system.
Temporary Licenses	Click to launch the Enable Temporary Licenses window. From this window, you can activate any available temporary licenses on the system.
Import	Click to read license information from a file (the default system license path is searched) and import the information into the system.

Add License Window

This window enables you to add a license with the specified parameters to the system.

The following table describes the fields and elements in this window.

TABLE F-73 Fields and Elements on the Add License Window

Field	Description
Module	The licensable module name.
Origination	The date on which the license becomes active, at 0000:00 hours.
Expiration	<p>The date on which the license expires, at 2359:59 hours.</p> <p>Note: Dates are specified in the format YYYYMMDD. The special date string 00000000 indicates that there is no restriction. If this string is used as the origination date, the license is active immediately; if it is used as the expiration date, the license never expires.</p>
Key	The license key, which must be in UUID format: XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXX.
Apply	Click to save your changes.

TABLE F-73 Fields and Elements on the Add License Window *(Continued)*

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Assign Language Panel

This panel enables you to specify the language displayed by the Web Administrator application. The application supports Unicode, officially known as the Unicode Worldwide Character Standard. This is a system for the interchange and display of international and classical languages.

Note: If you are accessing this panel through the configuration wizard, click Next to save your changes and proceed to the next panel in the wizard.

The following table describes the fields and buttons on this panel.

TABLE F-74 Fields and Elements on the Assign Language Panel

Field	Description
Codepage	Select a language codepage for the appliance or gateway-system server.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Enable Temporary Licenses Window

This window lets you enable the available temporary licenses for the system.

The following table describes the fields and elements in this window.

TABLE F-75 Fields and Elements on the Enable Temporary Licenses Window

Field	Description
Module	The licensable module name.

TABLE F-75 Fields and Elements on the Enable Temporary Licenses Window (*Continued*)

Field	Description
Duration	The number of days for which this temporary license will be enabled.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Import Licenses Window

This window enables you to import a license from a file.

Note: If you copy and paste, or manually enter the license information, please be sure you do not accidentally insert any line breaks within the license information. Otherwise, the lines will not be recognized as valid entries.

The following table describes the fields and elements in this window.

TABLE F-76 Fields and Elements on the Enable Temporary Licenses Window

Field	Description
Import License Field	The license information of the license you want to import.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.
Browse	Click to import the license from a file.

Set Administrator Password Panel

This panel enables you to set the system administrator password. In a cluster configuration, when you set the administrator password on one server (H1), the same password is propagated to the other server (H2).

The following table describes the fields and buttons on this panel.

TABLE F-77 Fields and Elements on the Set Administrator Password Panel

Field	Description
Old	The existing system administrator password. If there is no password, leave this field is blank.
New	The new system administrator password. The password must be at least one and no more than 20 characters long. If you want to disable the administrator password, leave this field blank.
Confirm	The new system administrator password, typed a second time.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Remote Access Panel

This panel enables you to set up network services that are used to remotely administer the NAS server. The following are the available network services:

- Telnet
- Remote Login
- Remote Shell
- Secure Shell, Web Admin (over Hypertext Transfer Protocol (HTTP))
- Secure Web Admin (over Secure Hypertext Transfer Protocol (HTTPS))

The following table describes the fields and buttons on this panel.

TABLE F-78 Fields and Elements on the Set Remote Access Panel

Field	Description
Secure Mode	Click to enable only those protocols that are deemed to be secure. This disables all other services. The following are the secure protocols: <ul style="list-style-type: none">• Secure Web Admin, which uses the Secure Socket Layer (SSL) over HTTP• Secure Shell (ssh)
Service	The existing services that are available to the NAS server.

TABLE F-78 Fields and Elements on the Set Remote Access Panel *(Continued)*

Field	Description
Enabled	Click to enable the corresponding service for remote access to the NAS server.
Comment	A line of text that describes the service.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Time and Date Panel

This panel enables you to set the server date and time.

The following table describes the fields, elements, and buttons on this panel.

TABLE F-79 Fields and Elements on the Set Time and Date Panel

Field	Description
Calendar	The current year, month, and day, in graphical format. To change the current year or month, select the options that you want from the appropriate drop-down menus on the calendar. To update the day, click the calendar itself.
Clock	The current time, in graphical format. To change the current time, select a new time from the drop-down menus located immediately above the clock. These drop-down menus display the time in military format (for example, 1:30 is displayed as 13:30).
Time Zone Drop-Down Menu	The current time zone where the server is located. To change the time zone, select a new time zone from the drop-down menu.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Time Synchronization Panel

This panel enables you to synchronize the NAS server time to either the Network Time Protocol (NTP) protocol or an RDATE server. NTP is an Internet protocol used to synchronize the clocks of computers to a reference time source, such as a radio, satellite receiver or modem. Typical NTP configurations use multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

The RDATE time protocol provides a site-independent date and time. It is a protocol that can retrieve the time from another machine on your network. RDATE servers are commonly present on Unix systems.

The following table describes the fields and buttons on this panel.

TABLE F-80 Fields and Elements on the Set Up Time Synchronization Panel

Field	Description
Manual Synchronization	Select to use neither NTP nor RDATE time synchronization.
NTP Synchronization	Select to use NTP synchronization, which requires that you have at least one NTP server on the network. The following options are specific to NTP synchronization: <ul style="list-style-type: none">• Enable Server 1, Enable Server 2 - Click either checkbox to enable that NTP server. Up to two NTP servers can be enabled.• NTP Server -The name or Internet Protocol (IP) address of the NTP server that the NAS server will poll for the current time.• Auth Type - Select the type of authentication to be used between the NAS server and the NTP server. Authentication support enables the NAS server to use a key and key identifier to verify that the NTP server is known and trusted. The NTP server and the NAS server must agree on the key and key identifier to authenticate their messages.

TABLE F-80 Fields and Elements on the Set Up Time Synchronization Panel (Continued)

Field	Description
	<ul style="list-style-type: none"> • Key ID – The key identifier that is associated with the private key from the <code>ntp . key</code> file that will be used with this NTP server. This field needs a value only if Symmetric Key was selected in the Auth Type field. The valid range for the Key ID value is 1 to 65534. Note: The <code>ntp . key</code> file must be copied to the <code>\etc</code> directory before symmetric key authentication is used. • Min Poll Rate – The minimum polling rate for NTP messages. This value to the power of 2 indicates the minimum number of seconds of the polling interval. For example, a value of 6 represents 36 seconds. The valid range for this field is 4 to 17. The default value of 6 is sufficient for most installations. • Max Poll Rate – The maximum polling rate for NTP messages. This value to the power of 2 indicates the maximum number of seconds of the polling interval. For example, a value of 4 represents 16 seconds. The valid range for this field is 4 to 17 but it must be larger than the minimum polling interval value. The default value of 10 is sufficient for most installations. • Enable Broadcast Client – Click to have the NAS server respond to NTP server broadcast messages received on any interface. This is intended for configurations involving one or more NTP servers with a large number of clients that require time synchronization from those servers. • Require Broadcast Server Authentication – Click to require the NTP client to verify that a server that has broadcast messages to the NAS server is a known and trusted server.
RDATE Synchronization	<p>Select to use the RDATE server time synchronization with the NAS server. The following options are specific to RDATE server synchronization:</p> <ul style="list-style-type: none"> • RDATE Server – The name or IP address of the RDATE server. • Tolerance – The maximum tolerance between the time on the NAS server and the time received from the RDATE server, between 0 and 3600 seconds. If the NAS server time is later or earlier than the RDATE server time by less than this number of seconds, the NAS server time will be synchronized with RDATE server time. If there is a larger discrepancy, the NAS server time will not be synchronized with the RDATE server. This validation occurs every day at 11:45 p.m.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Shut Down the Server Panel

This panel enables you to halt or reboot your NAS appliance or gateway server.

The following table describes the fields and buttons on this panel.

TABLE F-81 Fields and Elements on the Shut Down the Server Panel

Field	Description
None	Click to perform neither a shutdown nor a reboot of the server, or servers.
Halt both heads	Click to shut down both servers in a cluster configuration. Check to be sure both servers in the cluster are in the NORMAL state. To restart, you must manually power on the servers. This field is available only for dual-server cluster systems.
Reboot both heads	Click to shut down and restart both servers in a cluster configuration. This field is available only for dual-server (cluster) systems.
Halt	Click to shut down the server. To restart, you must manually power on the server. This field is available for single-server systems.
Reboot	Click to shut down and restart the server. This field is available for single-server systems.
Reboot Previous Version <i>version-number</i>	Select to shut down and restart the server, or servers, with an earlier version of the software. Use this option if you upgraded the software but encountered a problem. The server, or servers, is restarted with the last software used before the upgrade. In a cluster configuration, you must perform this action on each server in the cluster. Note: It is recommended that you check with Technical Support before choosing this option.
Halt this head	Click to shut down this server (the one to which you are currently logged on). The other server remains online. To restart, you must manually power on the server. This field is available only for dual-server systems.
Reboot this head	Click to shut down and restart this server (the one to which you are currently logged on). The other server remains online. This field is available only for dual-server systems.
Apply	Click to execute a server shutdown or reboot.

TABLE F-81 Fields and Elements on the Shut Down the Server Panel (Continued)

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel. Note: You cannot cancel a server shutdown or reboot after the shutdown or reboot has been initiated. Clicking Cancel only removes the entries you have typed on the panel.

Update Software Panel

This panel displays the current Sun StorageTek NAS software version on the server, and enables you to update the server with later versions of the software. You can update the server by downloading software from the Sun Microsystems web site and uploading it from your floppy or CD-ROM drive.

The following table describes the fields and buttons on this panel.

TABLE F-82 Fields and Elements on the Update Software Panel

Field	Description
The Current OS Version	The current version of NAS software running on the server.
<i>Update Server from a File</i>	
Path	The full path to the software file on your workstation. This file, which you can obtain from the Sun Microsystems web site, can be used to update the NAS software version on the server.
Browse	Click to locate the software file you want to install from your workstation.
Update	Click to execute the software upload from the file you have selected. When you have completed the upload process, the system prompts you to reboot the server. Click Yes to reboot, or No to continue without rebooting. The software update will not occur until you have rebooted the system.

Unix Configuration Panels

This section describes the fields and elements on the Unix Configuration panels:

- [“Add/Edit Comment Window” on page 432](#)
- [“Add/Edit Host Window” on page 433](#)
- [“Add/Edit NFS Export Window” on page 433](#)
- [“Add Hostgroup Member Window” on page 435](#)
- [“Add Hostgroup Window” on page 435](#)
- [“Configure Exports Panel” on page 436](#)
- [“Configure Name Services Panel” on page 437](#)
- [“Set Up FTP Panel” on page 439](#)
- [“Set Up Hostgroups Panel” on page 439](#)
- [“Set Up Local Hosts Panel” on page 440](#)
- [“Set Up NIS Panel” on page 441](#)
- [“Set Up NIS+ Panel” on page 442](#)
- [“Set Up NSSLDAP Panel” on page 443](#)

Add/Edit Comment Window

This window enables you to add or edit a comment about a Network File System (NFS) export, depending on how you accessed the window (by clicking the Add or Edit icon on the [“Configure Exports Panel” on page 436](#)).

The following table describes the fields and buttons in this window.

TABLE F-83 Fields and Elements on the Add/Edit Comment Window

Field	Description
Add Comment	Up to 80 characters of text describing an NFS export. You can start the comment text with the # character, or omit the # character to add a blank line.
Ok	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add/Edit Host Window

This window enables you to add or edit a host, depending on whether you accessed the window by clicking Add or Edit.



Caution: Exercise caution when granting trusted status to hosts. Trusted hosts have root access to the NAS file system, and can thus perform administrative functions in that file system.

The following table describes the fields and buttons in this window.

TABLE F-84 Fields and Elements on the Add/Edit Host Window

Field	Description
Host Name	The name of the host. The host name must begin with an alphabetic character or a number, and can include up to 63 alphanumeric characters, total: a–z, A–Z, 0–9, hyphens (-), and periods (.), but must not end with a hyphen or period character.
IP Address	The Internet Protocol (IP) address of the host.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit NFS Export Window

You can add and edit Network File System (NFS) exports from by clicking the Add or Edit icon on the [“Configure Exports Panel” on page 436](#) or by right-clicking a System Manager item and choosing the appropriate Add Export menu option.

You can only add NFS exports to whole volumes.

The following table describes the fields and buttons in this window.

TABLE F-85 Fields and Elements on the Add/Edit NFS Export Window

Field	Description
Volume	This field is available only if you clicked Add on the Configure Exports panel. Select the volume for which you are adding or editing an NFS export. You can only select whole volumes.

TABLE F-85 Fields and Elements on the Add/Edit NFS Export Window (*Continued*)

Field	Description
Path	This field is available only if you clicked Add on the Configure Exports panel. The directory for which you want to grant Unix NFS host access. Leaving this field blank exports the root directory of the volume.
Full Path	The full path to the exported directory on the volume.
<i>Access</i>	
Read/Write	Select to grant the specified hosts Read/Write permissions on the selected volume.
Read/Only	Select to grant the specified hosts Read/Only permissions on the selected volume.
No Access	Select to grant the specified hosts No Access permissions on the selected volume.
<i>Map Root User</i>	
Anonymous User	Select to map the user ID of root users to the user ID of anonymous users on this export.
Root User	Select to map the user ID of root users to the user ID of root (UID=0) on this export.
Map to UID	Select to assign a specific user ID to be used for root users on this export, and type the user ID.
<i>Hosts</i>	
Host Netgroups	This field is editable only in Add mode. Select to define the NFS export for a net group. From the drop-down menu, select the net group to which you want to assign the export.
Host Group	This field is editable only in Add mode. Select to define the NFS export for a host group. From the drop-down menu, select general (all hosts), trusted (all trusted hosts), or a user-defined host group.
Known Host	This field is editable only in Add mode. Select to define the export to a host that was added on the Set Up Local Hosts panel. From the drop-down menu, select the host to which you want to assign the export.
Other Host	This field is editable only in Add mode. Select to define the export to an individual host that you have not added through the Set Up Local Hosts panel. In the field to the right, type the name of the host.
Ok	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add Hostgroup Member Window

This window enables you to add members to the selected host group.

The following table describes the fields and buttons in this window.

TABLE F-86 Fields and Elements on the Add Hostgroup Member Window

Field	Description
Host Netgroups	Select this option and identify a Net group that is defined on an external NIS server to add as a member.
Host Group	Select this option and identify a host group to add as a member.
Known Host	Select a host that you have manually added on the Set Up Local Hosts panel or that exists on an external NIS server to add as a member.
Other Host	Type a host that is not available from the Set Up Local Hosts panel to add as a member.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Add Hostgroup Window

This window enables you to add a host group to the configuration.

The following table describes the fields and buttons in this window.

TABLE F-87 Fields and Elements on the Add Hostgroup Window

Field	Description
Add Hostgroup	The name of the host group that you want to add. The name must begin with a letter of the alphabet (a-z, A-Z), and can include up to 80 alphanumeric characters: a-z, A-Z, 0-9, hyphens (-), and periods (.), but must not end with a hyphen or period character.
Apply	Click to save your changes.

TABLE F-87 Fields and Elements on the Add Hostgroup Window (Continued)

Field	Description
Cancel	Click to clear the fields of new entries and close out of the window without saving any changes.

Configure Exports Panel

This panel enables you to specify access privileges for Unix users to specified volumes. The table on this panel shows the current Network File System (NFS) export information, including the accessible directories, host name, and access level (read/write or read/only) for each export.

Any host name beginning with @ represents a group of hosts. For instance, a host name of @general represents a predefined host group that includes all hosts. A host name of @trusted represents a predefined host group that includes trusted hosts.

Any host name beginning with & represents a host net group. For example, &group1 represents netgroup, group1.

The following table describes the fields and buttons on this panel.

TABLE F-88 Fields and Elements on the Configure Exports Panel









Field	Description
Full Path	The full path to the directory for which you want to grant Unix NFS access privileges.
Host	The name of the host, or hosts, that have access privileges on the volume.
Access	The level of access the host has on the volume. Access can be read/write (R/W) or read/only (R/O).
Map Root User	The method for mapping the user ID for root users. For more information, see “Creating Exports” on page 128 .
	Click to launch the Add NFS Export window. From this window, you can add a new NFS export to the configuration.
	Click to launch the Add Comment window. From this window, you can add a comment to the Configure Exports table.
	Click to launch the Edit NFS Export window or the Edit Comment window. From this window, you can edit the selected NFS export or comment.

TABLE F-88 Fields and Elements on the Configure Exports Panel *(Continued)*

Field	Description
	Click to delete the selected NFS export or comment from the table.
	Click to move the selected NFS export or comment to the top of the table.
	Click to move the selected NFS export or comment up one listing in the table.
	Click to move the selected NFS export or comment down one listing in the table.
	Click to move the selected NFS export or comment to the bottom of the table.

Configure Name Services Panel

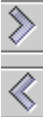

This panel enables you to specify the order in which name services (NS) are used for group, Net group, host, and user lookup functions. The NS lookup order controls the sequence in which the name services are searched to resolve a query. The supported name services are: NIS, NIS+, NSSLDAP, DNS, and Local. Before you can use a name service for name resolution, the service must be enabled.

The following table describes the fields and buttons on this panel.

TABLE F-89 Fields and Elements on the Configure Name Services Panel

Field	Description
Groups Order	Click to display the name services that are available to be searched for group lookup functions.
Netgroup Order	Click to display the name services that are available to be searched for Net group lookup functions.
Hosts Order	Click to display the name services that are available to be searched for user lookup functions.
Users Order	Click to display the name services that are available to be searched for host lookup functions.
Services Not Selected	The available name services that will not be used for lookup functions.

TABLE F-89 Fields and Elements on the Configure Name Services Panel (Continued)

Field	Description
	Click the top button to move the selected name service from the Services Not Selected list to Services Selected. Click the bottom button to move the selected name service from the Services Selected list to Services Not Selected.
Services Selected	The available services, in sequential order, that will be used for lookup functions. These services must be enabled.
	These buttons are available only if there is more than one name service in the Services Selected list. Click the top button to move the selected name service up in the list. Click the bottom button to move the selected name service down in the list.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Remove NFS Export Window

This window enables you to delete a Network File System (NFS) export from the configuration.

The following table describes the fields and buttons on this panel.

TABLE F-90 Fields and Elements on the Configure Exports Panel

Field	Description
Host	The name of the host, or hosts, that have access privileges on the volume.
Access	The level of access the host has on the volume. Access can be read/write (R/W) or read/only (R/O).
Apply	Click to delete the selected NFS export from the configuration.
Cancel	Click to exit out of the window without saving any changes.

Set Up FTP Panel

This panel enables you to set up File Transfer Protocol (FTP) service on the system and to define user access to the system by using FTP.

The following table describes the fields and buttons on this panel.

TABLE F-91 Fields and Elements on the Set Up FTP Panel



Field	Description
Enable FTP	Select to enable FTP on the system. If the FTP service is enabled, the FTP server accepts incoming connection requests.
Allow Guest Access	Select to enable access to the FTP server by anonymous users.
Allow User Access	Select to enable access to the FTP server by all users. If this checkbox is deselected, only <code>admin</code> and <code>root</code> users can access the FTP server.
Allow Admin Access	Select to enable access to the FTP server by all <code>root</code> users. A user is considered a root user if he or she is the special <code>admin</code> Sun StorageTek user or if his or her user identifier (UID) is equal to 0.
Enable Logging	Select to enable FTP logging.
Log File Name	This field is available only if logging is enabled. The name of the FTP log file.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up Hostgroups Panel

This panel enables you to monitor and manage the host groups database. Groups and group members can be added to or deleted from this database. Host groups are used to define a collection of hosts that can be used in Network File System (NFS) exports. Groups consist of predefined system groups and user-defined groups. The two predefined groups are the `Trusted` and `iso8859` groups.

The following table describes the fields and buttons on this panel.

TABLE F-92 Fields and Elements on the Set Up Hostgroups Panel

Field	Description
Groups	Select a group from the drop-down menu to display its members in the Group Members list.
	Click to launch either the Add Hostgroup or the Add Hostgroup Member window, depending on whether you click this button in the Groups or the Group Members section of the panel. For more information about adding new host groups or host group members, see “Adding a Host Group” on page 100 or “Adding a Member to a Host Group” on page 101 .
	Click to delete the selected host group or selected host group member, depending on whether you click this button in the Groups or the Group Members section of the panel.
Group Members	The members of the selected host group.

Set Up Local Hosts Panel

This panel enables you to add, edit, or remove host entries from the system host file.



Caution: Exercise caution in granting trusted status to hosts. Trusted hosts have root access to the NAS file system, and can therefore perform administrative functions in that file system.

The following table describes the fields and buttons on this panel.

TABLE F-93 Fields and Elements on the Set Up Local Hosts Panel

Field	Description
Host Name	The name of the host. The host name must begin with an alphabetic character or a number, and can include up to 63 alphanumeric characters, total: a–z, A–Z, 0–9, hyphens (-), and periods (.), but must not end with a hyphen or period character.
IP Address	The Internet Protocol (IP) address of the host.
New	Click to launch the Add Host window. From this window, you can add a host to the system host file.
Remove	Click to delete the host from the system host file.

TABLE F-93 Fields and Elements on the Set Up Local Hosts Panel (*Continued*)

Field	Description
Edit	Click to launch the Edit Host window. From this window, you can edit information about the selected host.

Set Up NIS Panel

This panel enables you to set up the Network Information Service (NIS) name service for the system. If you are running a pure Windows network, you do not need to set up NIS.

Note: If you are accessing this panel through the configuration wizard, make your changes and click Next to proceed to the next panel.

The following table describes the fields and buttons on this panel.

TABLE F-94 Fields and Elements on the Set Up NIS Panel

Field	Description
Enable NIS	Select to enable NIS, which configures the system to import the NIS database for host, user, and group information.
Domain Name	The name of the domain to be used for NIS services.
Server	The Internet Protocol (IP) address or name of the NIS server from which the NIS database is imported.
Check Rate	The frequency, in minutes, that NIS information is refreshed. The default is 5 minutes.
Use Broadcast	Select to acquire the NIS server name or IP address. This option is useful if you know the NIS domain name but not the NIS server name.
Update Hosts	Select to download the host information from the NIS server to the system.
Update Users	Select to download the user information from the NIS server to the system.
Update Groups	Select to download the group information from the NIS server to the system.
Update Netgroups	Select to download the Net group information from the NIS server to the system.
Apply	Click to save your changes.

TABLE F-94 Fields and Elements on the Set Up NIS Panel (*Continued*)

Field	Description
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up NIS+ Panel

This panel enables you to set up the Network Information Service Plus (NIS+) name service for the system. If you are running a pure Windows network, you do not need to set up NIS+.

Before enabling NIS+ on this panel, you must perform configuration steps on your NIS+ server. For more information, see [“Setting Up NIS+” on page 32](#).

The following table describes the fields and buttons on this panel.

TABLE F-95 Fields and Elements on the Set Up NIS+ Panel

Field	Description
Enable NIS+	Select to enable NIS+ on the system.
Home Domain Server	The name or Internet Protocol (IP) address of the NIS+ home domain server.
NIS+ Domain	The name of the NIS+ home domain.
Secure RPC Password	The password used by the system to enable communication with the NIS+ server.
Search Path	The domains that NIS+ searches through when looking for information. This field can be blank if you want NIS+ to search only the home domain and its parents. For example, if the NIS+ domain is <code>eng.sun.com</code> and the Search Path field is blank, the system first searches <code>eng.sun.com</code> then <code>sun.com</code> , and so on, when resolving names. Conversely, if the Search Path value is <code>sun.com</code> , the system searches only the domain <code>sun.com</code> when resolving names.
Use Broadcast	Select to acquire the NIS+ server name or IP address. This option is useful if you know the NIS+ home domain name but not the NIS+ server name.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Set Up NSSLDAF Panel

This panel enables you to set up Name Service Switch Lightweight Data Access Protocol (NSSLDAF), which is a Unix service that enables user account authentication.

The following table describes the fields and buttons on this panel.

TABLE F-96 Fields and Elements on the Set Up NSSLDAF Panel

Field	Description
Enable NSSLDAF	Select to enable NSSLDAF for the system.
Domain (DN)	The Lightweight Data Access Protocol (LDAP) domain name, in domain name (DN) or LDAP format.
Password	The bind password on the NSSLDAF server.
Server	The Internet Protocol (IP) address of the NSSLDAF server.
Proxy (DN)	The NSSLDAF proxy (entryDN).
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Windows Configuration Panels

This section describes the fields and elements on the Windows Configuration panels:

- [“Add/Edit Group Panel” on page 444](#)
- [“New Share Window” on page 444](#)
- [“Edit Share Window” on page 446](#)
- [“Add/Edit SMB/CIFS User or Group Map Window” on page 449](#)
- [“Configure Autohome Panel” on page 450](#)
- [“Configure Domains and Workgroups Panel” on page 452](#)
- [“Configure Groups Panel” on page 454](#)
- [“Configure Mapping Policy Panel” on page 455](#)
- [“Configure Maps Panel” on page 456](#)
- [“Configure Shares Panel” on page 457](#)

- “Remove Share Window” on page 459
- “Set Up WINS Panel” on page 459
- “System Status Panel” on page 460

Add/Edit Group Panel

This window enables you to add or edit a group, depending on whether you accessed the window by clicking Add Group or Edit Group.

The following table describes the fields and buttons in this window.

TABLE F-97 Fields and Buttons on the Add/Edit Group Window

Field	Description
Group	The name of the group.
Comment	(Optional) A brief line of text that describes the group.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

New Share Window

You can add shares from two places in the Web Administrator GUI:

- From the Configure Shares panel, by selecting New.
- From the System Manager panel, by selecting a volume or directory and choosing the appropriate option from the right-click menu (Sharing > New Share).

Use the New Share window to specify or modify a static Server Message Block (SMB) share, depending on whether you accessed the window in Add or Edit mode.

The following table describes the fields and buttons in this window.

TABLE F-98 Fields and Buttons on the New Share Window

Field	Description
Share Name	<p>Name of the share. This is the name that users will see on the network.</p> <p>The share name can be up to 15 characters in length, and can include any alphanumeric characters except those listed below: " / \ [] : < > + ; , ? * =</p>
Comment	<p>(Optional) Brief line of text that describes the share. You can enter up to 60 alphanumeric characters.</p>
Mac Extensions	<p>Select this Desktop DB Calls checkbox to allow the system to access and set Macintosh desktop database information. Enabling this option speeds up Macintosh client file access on the NAS appliance or gateway-system, and allows non-Macintosh clients to access Macintosh files.</p>
Volume Name	TBS
Directory	TBS
Container	<p>Applicable only if Active Directory Service (ADS) is enabled for the share, as described under “Configure Domains and Workgroups Panel” on page 452. Specify the location in the ADS directory where the share will be published.</p> <p>Type the container information following LDAP DN (Lightweight Directory Access Protocol, distinguished name) notation. Objects, such as users and shares, are located in Active Directory domains according to a hierarchical path, which includes each level of “container” objects.</p> <p>Type the path in terms of the <code>cn</code> (common name) folder or <code>ou</code> (organizational unit) of the share. Do not include the domain name in the path. The <code>cn</code> containers are default folders in the <code>root</code> folder. All other containers are <code>ou</code> folders. For example, if the share will reside in a <code>shares</code> organizational folder within an organizational parent folder called <code>accounting</code>, you would type the following: <code>ou=shares,ou=accounting</code></p>
Virus Scan Exempt	Select to exempt the share from antivirus scan..

TABLE F-98 Fields and Buttons on the New Share Window *(Continued)*

Field	Description
User ID	<p>This field is applicable only if Windows Workgroup mode (not NT Domain mode) is enabled, as described under “Configure Domains and Workgroups Panel” on page 452. Together with the Group ID field, it provides the sole means of security for NAS file ownership and access by Windows Workgroup users.</p> <p>User identification (UID) of the user accessing the volume/directory through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.</p>
Umask	<p>This field is applicable only if Windows Workgroup mode is enabled. Access permissions for the share, specified as a three-digit number. For detailed information about access permissions for shares, see “About Share Access Permissions” on page 115.</p>
R/W Password	<p>This field is available only if Windows Workgroup mode is enabled. Password for Windows Workgroup users who will have read/write access to the share.</p>
R/O Password	<p>This field is available only if Windows Workgroup mode is enabled. The password for Windows Workgroup users who will have read-only access to the share.</p>
Group ID	<p>This field is applicable only if Windows Workgroup mode is enabled. Group identification (GID) of the user accessing the volume/directory through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.</p>
Confirm R/W Password	<p>Same as the R/W Password field, for confirmation.</p>
Confirm R/O Password	<p>Same as the R/O Password field, for confirmation</p>
Apply	<p>Click to save your changes.</p>
Cancel	<p>Click to clear the fields of new entries and return to the values that were originally displayed in the window.</p>

Edit Share Window

You can edit shares from two places in the Web Administrator GUI:

- From the Configure Shares panel, by selecting Edit.
- From the System Manager panel, by selecting a volume or directory and choosing the appropriate option from the right-click menu (Sharing > Edit Share).

Use the Edit Share window to specify or modify a static Server Message Block (SMB) share, depending on whether you accessed the window in Edit mode.

The following table describes the fields and buttons in this window.

TABLE F-99 Fields and Buttons on the Edit Share Window

Field	Description
Old Share Name	Display-only, and applicable only in Edit mode. Current name of the share.
Share Name	Name of the share. This is the name that users will see on the network. The share name can be up to 15 characters in length, and can include any alphanumeric characters except those listed below: " / \ [] : < > + ; , ? * =
Comment	(Optional) Brief line of text that describes the share. You can enter up to 60 alphanumeric characters.
Mac Extensions	Select this Desktop DB Calls checkbox to allow the system to access and set Macintosh desktop database information. Enabling this option speeds up Macintosh client file access on the NAS appliance or gateway-system, and allows non-Macintosh clients to access Macintosh files.
Path	Applicable only if you requested this screen for Add processing from the System Manager. Path (volume name and directory, as applicable) you want to share. Display-only for Add processing. Editable for Edit processing.

TABLE F-99 Fields and Buttons on the Edit Share Window (Continued)

Field	Description
Container	<p>Applicable only if Active Directory Service (ADS) is enabled for the share, as described under “Configure Domains and Workgroups Panel” on page 452. Specify the location in the ADS directory where the share will be published.</p> <p>Type the container information following LDAP DN (Lightweight Directory Access Protocol, distinguished name) notation. Objects, such as users and shares, are located in Active Directory domains according to a hierarchical path, which includes each level of “container” objects.</p> <p>Type the path in terms of the <code>cn</code> (common name) folder or <code>ou</code> (organizational unit) of the share. Do not include the domain name in the path. The <code>cn</code> containers are default folders in the <code>root</code> folder. All other containers are <code>ou</code> folders. For example, if the share will reside in a <code>shares</code> organizational folder within an organizational parent folder called <code>accounting</code>, you would type the following: ou=shares,ou=accounting</p>
Virus Scan Exempt	Select to exempt the share from antivirus scan.
User ID	<p>This field is applicable only if Windows Workgroup mode (not NT Domain mode) is enabled, as described under “Configure Domains and Workgroups Panel” on page 452. Together with the Group ID field, it provides the sole means of security for NAS file ownership and access by Windows Workgroup users.</p> <p>User identification (UID) of the user accessing the volume/directory through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.</p>
Umask	<p>This field is applicable only if Windows Workgroup mode is enabled. Access permissions for the share, specified as a three-digit number. For detailed information about access permissions for shares, see “About Share Access Permissions” on page 115.</p>
R/W Password	<p>This field is available only if Windows Workgroup mode is enabled. Password for Windows Workgroup users who will have read/write access to the share.</p>
R/O Password	<p>This field is available only if Windows Workgroup mode is enabled. The password for Windows Workgroup users who will have read-only access to the share.</p>

TABLE F-99 Fields and Buttons on the Edit Share Window *(Continued)*

Field	Description
Group ID	This field is applicable only if Windows Workgroup mode is enabled. Group identification (GID) of the user accessing the volume/directory through this share. The default value for this field is 0 (zero), which is the value of the Unix root user. Use caution when assigning a zero value, however. In Windows Workgroup mode, typing zero in this field disables all security on all files and directories in the share.
Confirm R/W Password	Same as the R/W Password field, for confirmation.
Confirm R/O Password	Same as the R/O Password field, for confirmation.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Add/Edit SMB/CIFS User or Group Map Window

This window enables you to add or edit the SMB/CIFS user or group map, depending on whether you accessed the window by clicking Add or Edit on the [“Configure Maps Panel” on page 456](#).

The following table describes the fields and buttons in this window.

TABLE F-100 Fields and Buttons on the Add/Edit SMB/CIFS User or Group Map Window

Field	Description
<i>NT Group</i>	
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.
<i>Unix Group</i>	
Name	The Unix user or group name to which you want to map the specified NT user or group.

TABLE F-100 Fields and Buttons on the Add/Edit SMB/CIFS User or Group Map Window

Field	Description
ID	The identifier that uniquely identifies the Unix user or group within the Unix domain.
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed in the window.

Configure Autohome Panel

This panel enables you to configure temporary shares, created when a user logs in to the system and then removed when the user logs out. The mapping file `/dvol/etc/autohome.map` contains the rules and search options for determining whether to share a home directory when a Windows client connects to the server.






For more information, see [“About Autohome Shares” on page 119](#).

The following table describes the fields and buttons on this panel.

TABLE F-101 Fields and Buttons on the Configure Autohome Panel

Field	Description
<i>Default Rule</i>	Select one of these rules to be used when no Specific Rule is defined or no Specific Rule maps to a user name.
Use Wildcard	Click to allow a share with any user name
Use Name Services	Click to allow a share with a user name if the user name matches an entry in either NIS or NIS+, based on lookup order. See (Set Up NIS, Setup NIS+, Configure Name Services). If there is no match, the share is not allowed.
No Default Rule	Click to require a match with one of the user names as defined by a Specific Rule.
<i>Specific Rules</i>	The list of rules that operate to allow a share with a user name. These rules take precedence over the default rules. Each rule consists of a Name, a Home Directory, and an ADS Container if enabled.
Name	Valid user name

TABLE F-101 Fields and Buttons on the Configure Autohome Panel (Continued)

Field	Description
Home Directory	<p>The absolute directory path for the user name in the Name field. For example, if a user's home directory is <code>/vol1/fort/tom</code>, the Home Directory field contains <code>/vol1/fort</code>. The following substitutions can be used for the user name:</p> <ul style="list-style-type: none">• Question mark (?) substitutes for the first character of the user name• Ampersand (&) substitutes for the whole user name <p>For example, if a Home Directory is defined as <code>/vol1/fort/?/&</code>, the directory resolves to <code>/vol1/fort/t/tom</code></p> <p>For more information about how to specify valid values in this field, see "About Autohome Shares" on page 119.</p>
ADS Container	<p>(Available if ADS is enabled. See "Configure Domains and Workgroups Panel" on page 452) Specifies the Active Directory Service (ADS) container in which the temporary shares can be published. For more information about how to specify valid values in this field, see "About Autohome Shares" on page 119.</p>
	<p>Use these controls to change the order of the rules in the list. Select a rule to highlight and then click on the arrow button to move the rule.</p>
	
	<p>Click to add a new rule to the Specific Rules. This opens the Add Rule dialog.</p>
	<p>To change a rule, select the rule and then click the Edit button. The Edit Rule dialog is displayed.</p>
	<p>To remove a rule, select the rule and then click the Delete button.</p>
Apply	<p>Click to save your changes.</p>
Cancel	<p>Click to clear the fields of new entries and return to the values that were originally displayed on the panel.</p>

Add/Edit Rule

Use this panel to define a rule in the mapping file `/dvol/etc/autohome.map`, used for determining whether to share a home directory when a Windows client connects to the server.

For more information, see [“Configure Autohome Panel” on page 450](#).

The following table describes the fields and buttons on this panel.

TABLE F-102 Fields and Buttons on the Configure Autohome Panel

Field	Description
Name	Enter a valid user name
Home Directory	Enter the absolute directory path for the user name, starting with the volume name up to the user name. For example, if a user's home directory is <code>/vol1/fort/tom</code> , the Home Directory field contains <code>/vol1/fort</code> . You can use following characters to substitute for the user name: <ul style="list-style-type: none">• Question mark (?) substitutes for the first character of the user name.• Ampersand (&) substitutes for the whole user name. For example, if a Home Directory is defined as <code>/vol1/fort/?/&</code> , the directory resolves to <code>/vol1/fort/t/tom</code> For more information about how to specify valid values in this field, see “About Autohome Shares” on page 119 .
ADS Container	(Available if ADS is enabled. See “Configure Domains and Workgroups Panel” on page 452) Specifies the Active Directory Service (ADS) container in which the temporary shares can be published. For more information about how to specify valid values in this field, see “About Autohome Shares” on page 119 .
OK	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Domains and Workgroups Panel

This panel enables you to configure Windows networking for either a Windows NT Domain or a Workgroup security model.

Note: If the security model changes between the Windows Workgroup and NT Domain model, a confirmation message prompts you to confirm an automatic server reboot. Click Yes to reboot the system.

The following table describes the fields and buttons on this panel.

TABLE F-103 Fields and Buttons on the Configure Domains and Workgroups Panel

Field	Description
<i>Domain</i>	
Domain	<p>Name of an existing domain. Domain names must not exceed the 15-character NetBIOS limit.</p> <p>Note: If you want to enable Active Directory Service (ADS), type the name of the Windows 2000 domain in which ADS is running. The system must also belong to this domain.</p>
User Name	<p>Name of an existing domain user.</p> <p>If you want to enable ADS, the user name in this field must be for a Windows 2000 user with administrative rights. This user must be the domain administrator or a user that is a member of the domain Administrators group. The ADS client performs secure ADS updates with this user.</p> <p>Note: If the domain administrator user name is displayed in this field but the ADS update fails, the domain administrator password must be changed (on the domain controller). This is only required for the administrator user, and the same password can be reused. For more information, see the Microsoft Support Services Web Site, Article Q248808.</p>
Password	<p>Password of the domain user. For ADS, this is the Windows administrative user's password.</p>
Enable ADS	<p>Select if you want the Active Directory Service (ADS) software to publish Sun StorageTek shares to ADS, or remove Sun StorageTek shares from ADS. For more information about ADS and how to configure it, see "About Active Directory Service" on page 86.</p>
ADS Information	<p>Information specific to the Active Directory Service:</p> <ul style="list-style-type: none">• Container - The ADS path location of the Windows 2000 administrative user in Lightweight Directory Access Protocol (LDAP) distinguished name (DN) notation. Type 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 <p>Note: Do not include the domain name in the path.</p> <ul style="list-style-type: none">• Site - If the ADS domain controller is in a different subnet than the client, type 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.

TABLE F-103 Fields and Buttons on the Configure Domains and Workgroups Panel

Field	Description
Kerberos Domain Information	Information specific to the Kerberos domain: <ul style="list-style-type: none">• Realm - The Kerberos realm name that is used to identify ADS (this is usually the ADS domain). This is usually the ADS domain or the Domain Name Service (DNS) domain. When you click Apply, this entry is converted to all uppercase letters.• Server - The host name of the Kerberos Key Distribution Center (KDC) server. This is usually the host name of the primary domain controller in the ADS domain. If the software can locate the KDC server by using Domain Name Service (DNS) software, this field will be blank.
<i>Workgroup</i>	
Name	Name of the workgroup.
Comments	Line of text that describes the network configuration.
Apply	Click to save your changes. If you are configuring Windows networking for a Windows NT domain, an account is created on the domain for this system.
Cancel	Click to clear the fields of new entries and to return the values that were originally displayed on the panel.

Configure Groups Panel

This panel enables you to administer local groups. Privileges are granted to individual local groups rather than to individual users.

Note: Local groups apply only to environments that use Common Internet File System (CIFS) networking. For more information about local groups, see [“About Local Groups” on page 94](#).

The following table describes the fields and elements on this panel.

TABLE F-104 Fields and Elements on the Configure Groups Panel

Field	Description
Groups	The groups of which the system is aware. When you select a group from this list, the Group Members and the Group Privileges lists are updated with information specific to that group.

TABLE F-104 Fields and Elements on the Configure Groups Panel (Continued)

Field	Description
Group Members	The users that are members of the selected group. For information about adding and removing users to and from a group, see “Adding and Removing Group Members and Configuring Privileges” on page 96.
Group Privileges	The privileges that are applied to the selected group. For more information about the supported group privileges, see “About Configuring Privileges for Local Groups” on page 94
Comment	A line of text that describes the group.
Apply	Click to save your changes.
Add Group	Click to launch the Add Group window. From this window, you can create a new group. For more information, see “Adding and Removing Group Members and Configuring Privileges” on page 96.
Edit Group	Click to launch the Edit Group window. From this window, you can edit the name and comment text for the selected group. You cannot edit the following default groups: Administrators, Backup Operators, and Power Users.
Remove Group	Click to delete the selected group. You cannot delete the following default groups: Administrators, Backup Operators, and Power Users.
Refresh	Click to update the panel with the latest information. Note: If you have made changes but you have not yet clicked Apply, clicking Refresh removes your changes from the panel.

Configure Mapping Policy Panel

If your system includes both Unix and Windows environments, this panel enables you to establish rules for an equivalence relationship between Unix users and groups and Windows users and groups.

Choosing a user and group mapping policy establishes credential equivalence on the NAS appliance or gateway system, to provide common access using either environment. For more information, see [“About Mapping User and Group Credentials”](#) on page 102.

The following table describes the fields and buttons on this panel.

TABLE F-105 Fields and Elements on the Configure Mapping Policy Panel

Field	Description
<i>Windows <__> Unix User Mapping Choice</i>	
Default Mapping	Select to establish no predefined mapping rule between Windows and Unix users. New users are assigned newly-generated, unique user identifiers by the system.
Map by User Name	Select to map Unix and Windows users who have identical user names. This enables a user to access the NAS appliance or gateway system from both environments.
Map by Full Name	Select to map Unix and Windows users that have identical full names.
<i>Windows <__> Unix Group Mapping Choice</i>	
Default Mapping	Select to establish no predefined mapping rule between Windows and Unix groups. New groups are assigned newly-generated, unique, group identifiers by the system
Map by Group Name	Select to map Unix and Windows groups that have identical group names.
Map to Primary Group	Select to map to the NFS group in the primary group field in the configured <code>passwd</code> file. For more information, see “About Group Mapping” on page 106 .
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

Configure Maps Panel

This panel enables you to view existing mappings between Unix users and groups and Windows users and groups. It also enables you to manually configure mappings between Unix users and groups and Windows users and groups.

The following table describes the fields and buttons on this panel.

TABLE F-106 Fields and Elements on the Configure Maps Panel

Field	Description
Users	Select to display existing user mappings in the table.
Groups	Select to display existing group mappings in the table.
Unix Name	The name of the user or group as defined in the Unix environment.
Unix ID	The unique identifier assigned to the user or group in the Unix environment.
Windows Name	The name of the user or group as defined in the Windows environment.
Windows Domain	The domain to which the user or group belongs in the Windows environment.
Windows RID	The relative identifier (RID) assigned to the user or group in the Windows environment.
Add	Click to launch the Add SMB/CIFS User Map window or the Add SMB/CIFS Group Map window, depending on whether you selected Users or Groups at the top of the Configure Maps panel. From this window, you can configure a new user or group mapping. For more information, see “Mapping Windows Groups and Users to Unix Groups and Users” on page 109.
Remove	Click to delete the selected user or group mapping, depending on whether you selected Users or Groups at the top of the Configure Maps Panel.
Edit	Click to launch the Edit SMB/CIFS User Map window or the Edit SMB/CIFS Group Map window, depending on whether you selected Users or Groups at the top of the Configure Maps panel. From this window, you can edit the selected user or group mapping. For more information, see “Editing a Mapping Between a Windows Group or User and a Unix Group or User” on page 110.

Configure Shares Panel

This panel displays the current Server Message Block (SMB) shares and their attributes. Use this panel to create new shares, change the attributes of an existing share, or delete a share.

Note: After creating a volume, you must create a share for the volume. Users can then access the volume and create directories. After directories are created on the volume, you can create individual shares for them.

The following table describes the fields and buttons on this panel.

TABLE F-107 Fields and Buttons on the Configure Shares Panel

Field	Description
Name	Name of the share.
Path	Location of the share on the system.
Virus Scan	Displays whether the share is scanned for viruses.
Comment	Text description relating to the share (can be blank).
User	Applicable only if Windows Workgroup mode is enabled, as described under “Configure Domains and Workgroups Panel” on page 452 . User identification (UID) of the user accessing the volume/directory through this share.
Group	Applicable only if Windows Workgroup mode is enabled. Group identification (GID) of the user accessing the volume/directory through this share.
Umask	Applicable only if Windows Workgroup mode is enabled. Access permissions for the share, specified as a three-digit number. For detailed information about access permissions for shares, see “About Share Access Permissions” on page 115 .
Container	Applicable only if Active Directory Service (ADS) is enabled for the share, as described under “Configure Domains and Workgroups Panel” on page 452 . ADS container in which the share is published.
Desktop DB Calls	Whether the system can access and set Macintosh desktop database information. If the On value is displayed in this field, Macintosh client file access is sped up and non-Macintosh clients can access Macintosh files in this share.
New	Click to open the New Share window and add a new share.
Remove	Click to remove the selected share. Click Yes on the verification screen to remove the share.
Edit	Click to open the Edit Share window and modify the selected share.

Remove Share Window

This window displays when you request removal of a share from the System Manager. Use it to remove a static Server Message Block (SMB) share.

The following table describes the fields and buttons in this window.

TABLE F-108 Fields and Elements on the Remove Share Window

Field	Description
Name	Name of the share.
User	Applicable only if Windows Workgroup mode is enabled, as described under “Configure Domains and Workgroups Panel” on page 452. User identification (UID) of the user accessing the volume/directory through this share.
Group	Applicable only if Windows Workgroup mode is enabled. Group identification (GID) of the user accessing the volume/directory through this share.
Apply	Click to remove the share.
Cancel	Click to exit out of the window without removing the share.

Set Up WINS Panel

If you are using a Windows or a mixed environment, this panel enables you to set up the Windows Internet Naming Service (WINS) server with the NAS software.

The WINS server enables computers on your network to communicate with each other by resolving Network Basic Input/Output System (NetBIOS) names to Internet Protocol (IP) addresses. If Server Message Block (SMB) is enabled, your system has a NetBIOS name.

If you are using a pure Unix environment, you do not need to set up WINS.

The following table describes the fields and buttons on this panel.

TABLE F-109 Fields and Buttons on the Set Up WINS Panel

Field	Description
Enable WINS	Select to enable WINS, which allows the system to be a WINS client.
Primary WINS Server	The IP address of the server that is consulted first for NetBIOS name resolution.
Secondary WINS Server	The IP address of the server that is consulted only if the primary WINS server is not responding.
Scope	A valid domain name as defined by the Domain Name Service (DNS) software. Defining a scope prevents this computer from communicating with any systems that do not have the same scope configured. Therefore, use caution 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. For more information about valid values that you can enter in this field, see “Setting Up WINS” on page 29 .
Apply	Click to save your changes.
Cancel	Click to clear the fields of new entries and return to the values that were originally displayed on the panel.

System Status Panel

This panel enables you to view general information about the network attached storage (NAS) system. In the bottom portion of the panel, the latest status of the system is displayed.

The following table describes the fields on this panel.

TABLE F-110 Fields on the System Status Panel

Field	Description
Name	Name of the NAS server.
Model	Server model number.
Serial #	Unique serial number of the system.
Up Time	Amount of time elapsed since the system was last turned on.

TABLE F-110 Fields on the System Status Panel (*Continued*)

Field	Description
CPU Load	Current and peak central processing unit (CPU) load.
OS Version	Current version of NAS software running on the server.
Web Administrator Version	Version designation for the graphical Web Administrator application.

Index

A

- access list 289
 - iSCSI 289
- access rights, defined 95
- Active Directory Service
 - see ADS
- active server
 - configuring 135
 - defined 133
- activity monitor 284
- adapters, network 244
 - configuring 25
- adding
 - checkpoints 177, 296
 - directory tree quotas 125
 - file volume 254
 - group members 96, 262
 - group quotas 123
 - hosts 98, 268
 - LUN 47
 - NFS exports 128
 - RAID 47
 - segment 255
 - shares 258
 - static shares 116, 118, 119
 - trusted hosts 98, 269
 - user groups 262
 - user quotas 123
- admin command 242
- administration console 241
 - keys 243
 - main menu 243
- administrator
 - group 94
- administrator password 245
- ADS
 - configuring 87
 - Windows 2000 clients 119
 - container names 88
 - defined 86
 - enabling 87
 - overview 87
 - publishing shares 90
 - removing shares 91
 - setting up 29, 87, 260
 - updating share containers 90
- aggregating
 - see bonding ports
- alert
 - mirror buffer thresholds 140
- alias IP address
 - defined 78
- allows 161
- antivirus scan 72, 248
- appliances
 - overview 338–339
- assigning
 - hot-spare 49
 - port roles 26
- attaching segments 255
- audit 161, 298
 - setting up 162
 - system 161
- autohome shares 257

- configuring 120
- defined 119

B

- back-end storage
 - overview 339
- backup
 - NDMP 186, 296
 - operators group 94
- bezel 221
- bonding ports 79
 - dual-server systems 81
 - viewing 285
- breaking mirrors 141, 145, 276, 279

C

- cable
 - USB-to-serial port 339
- CATIA V4/V5 189
- changing
 - directory tree quotas 126
 - group quotas 124
 - hosts 98, 268
 - name services lookup order 92
 - NFS exports 129
 - scheduled checkpoint 179
 - static shares 118, 259
 - user quotas 124
- channel bonding
 - see bonding ports
- character translations 189
 - for Korean euc-kr filenames 59, 100
 - for Windows Unicode 59
- checkpoints
 - accessing 183
 - adding to schedule 296
 - analysis 285
 - creating 177
 - defined 176
 - editing the schedule 179
 - enabling 177
 - NDMP 176
 - removing 180, 181
 - renaming 181
 - scheduling 178, 296
 - sharing 182
- chsmb command 267

CIFS

- autohome shares 120
- Compliance Archiving Software 194
- configuring clients
 - DOS 119
 - Windows 119
- defined 114
- drive letter mapping 253
- static shares 256
 - adding 116, 118, 119
 - configuring 116
 - creating 116
 - defined 114
 - editing 118
 - removing 118
 - security 117
- clients
 - configuring 119
 - DOS 119
 - Windows 119
- cluster
 - enabling head failover 21
 - naming volumes 51
 - port roles 26
 - power cycling single controller 22
 - reset due to power failure 326
 - software serial number 320
- command line 241
 - security 242
- commands 242
 - admin 242
 - chsmb 267
 - man 244
 - menu 243
 - raidctl profile 205
 - umask 117
- Common Internet File System
 - see CIFS
- Compatibility level 175
- Compliance Archiving Software 147
 - advisory enforcement 149
 - API 305
 - configuring 194
 - mandatory enforcement 148
- configuration
 - controller and expansion units 335
 - minimum 339
- configure 290

- configuring
 - active server 135, 272, 273
 - ADS 29, 87, 260
 - antivirus 72
 - antivirus scan 248
 - autohome shares 120, 257
 - Compliance Archiving Software 194
 - date 70, 245
 - directory tree quotas 125
 - DNS 30, 250
 - drive letters 253
 - email notification 281
 - failback 295
 - failover 294
 - FTP 172, 293
 - gateway address 27
 - group
 - quotas 122
 - group maps 265
 - group privileges 94
 - hosts 98
 - iSCSI target 59, 60, 288
 - language 36, 249
 - LDAP 91
 - local logging 250
 - logging 35
 - mirror server 135, 272, 273
 - mirroring 272, 273
 - mirroring file volumes 136, 274
 - name service 252
 - name services 34, 250
 - NDMP 186, 187, 296
 - network adapters 25
 - NFS exports 128
 - NICs 25
 - NIS 31, 251
 - NIS+ 32
 - NTP 69, 246
 - ports 25, 244
 - mirroring 135
 - privileges 97
 - RDATE 69, 246, 248
 - remote logging 250
 - secure clock 246
 - server name 16
 - shares 256
 - SMB/CIFS clients 119
 - SNMP 156, 281
 - starting the wizard 12
 - static shares 116
 - system audit 162
 - target server 135
 - TCP/IP 244
 - time 70, 245
 - time synchronization 69, 246
 - time zone 70, 245
 - user group privileges 263
 - user groups 262
 - user maps 264
 - user quotas 122
 - variations of the wizard 11
 - verifying DNS for ADS 89
 - warning thresholds 140
 - warnings 275
 - Windows security 28
 - WINS 29
 - wizard 11
- console 241
 - locking 271
 - main menu 243
 - unlocking 271
- containers, updating ADS shares 90
- content panel 8
- controller
 - information, viewing 169
- controller unit
 - supported drives 328
- controller units 339
 - location 174
- conventions
 - server names 16
- cover 220
 - front 223
- creating
 - checkpoints 177, 296
 - directory tree quotas 125
 - file volume 50, 254
 - group quotas 123
 - hosts 98, 268
 - LUN 47
 - LUNs 47
 - NFS exports 128
 - RAID 47
 - scheduled checkpoint 296
 - segment 50, 255
 - static shares 116, 258
 - trusted hosts 98, 269

- user quotas 123
- creating a file system 46
- credentials, mapping 102
- CRU
 - locations 224
- CRUs,defined 217

D

- date 70, 245
- dedicated port
 - mirroring 135
 - setting port role 135
- default quotas
 - group 122
 - user 122
- defining
 - file volume 50
 - LUNs 47
 - RAID 47
 - segment 50
- deleting 256
 - checkpoint 181
 - directory tree quotas 127
 - file volume 256
 - hosts 99
 - NFS exports 130
 - out-of-date file volume 145, 279
 - static shares 118, 260
 - trusted hosts 99, 269
 - user quotas 124
- deleting scheduled checkpoints 180
- DHCP
 - disabling with head failover 22
- diag.tar.gz 282
- diagnostic email 282, 341
- DIMM 231
- directory tree quotas
 - adding 125
 - configuring 125
 - defined 125
 - deleting 127
 - editing 126
- disk
 - location 174
- disk failure
 - identifying 337

- disk volume 256
- Display System Log 158
- displaying
 - routes 167
 - system events 159
 - system log 158, 160
- DNS
 - defined 86
 - Dynamic DNS 250
 - setting up 30, 250
 - verifying configuration 89
- domain
 - security 28
- DOS, configuring for SMB/CIFS 119
- down timeout, defined 23
- drive
 - location 174
- drive failure
 - identifying 337
- drive firmware, upgrading 195
- drive letters 253
- drive shuttle
 - replacing 336
- DTQ
 - see directory tree quota
- Dual-port Fibre Channel card 236
- dual-server systems
 - bonding ports 81
 - enabling head failover 21, 294
 - IP address aliases 78
 - port roles 26
- dynamic DNS
 - enabling 30

E

- editing
 - directory tree quotas 126
 - group maps 265
 - group quotas 124
 - hosts 98, 268
 - LUN path 295
 - NFS exports 129
 - scheduled checkpoint 179
 - static shares 118, 259
 - user maps 264
 - user quotas 124

- email notification
 - configuring 281
 - diagnostic 341
 - notification levels 35
 - sending diagnostic message 282

- enabling
 - ADS 87
 - autohome shares 120
 - checkpoints 177, 296
 - controller failover 294
 - DNS 30
 - domain security 28
 - dynamic DNS 30
 - failover 21
 - group quotas 123
 - head failover 294
 - LDAP 91
 - link failover 23, 294
 - logging 35
 - name services 34
 - NIS 31
 - NIS+ 32
 - quotas 261
 - static shares 116
 - UPS monitoring 168
 - user quotas 123
 - WINS 29

- environmental status
 - system fans 163
 - system power supplies 163
 - temperature 163
 - viewing 163
 - voltage 164

- error messages 299
 - file system 302
 - IPMI events 303
 - RAID subsystem errors 302
 - SysMon 300
 - UPS 300

- events
 - auditing 161, 298
 - environment 303
 - logging 251
 - system log 159

- expansion units
 - location 174
 - overview 339

- exports

- creating 128
- editing 129
- removing 130
- setting up 128

F

- failback
 - configuring 295
 - defined 22
 - initiating 24

- failover
 - configuring 294
 - defined 22
 - enabling 21
 - link 23

- fan connector board 225

- fan status 163

- fan tray assembly 233

- fan tray fault LED (rear) 324

- Fibre Channel drives 335

- file directory security 111

- File Replicator 133

- file system

- creating 46

- error messages 302

- managing 253

- File Transfer Protocol

- see FTP

- file volume

- autohome shares

- defined 119

- creating 50, 254

- defined 45

- deleting 256

- deleting out-of-date volume 145

- expanding 255

- managing access 270

- mirroring 136, 274

- mirroring up-to-date volume 145, 280

- name limits 51

- promoting 142, 277

- re-establishing mirror 144, 278

- static shares

- defined 114

- usage statistics 165

- file volumes

- mirroring 274

- firmware
 - directories and files 198
 - revision level 195
 - upgrading with reboot 196, 204
 - upgrading without reboot 199
- front panel
 - buttons 323
 - indicator board 227
- FTP
 - access 173
 - configuring 172, 293
 - user types 292

G

- gateway address 27
- GID, defined 117
- Gigabit Ethernet
 - copper 338
 - fiber 338
- group 262
 - adding members 96, 262
 - administrators 94
 - backup operators 94
 - credentials, mapping 102
 - power users 94
 - privileges 94
 - quotas
 - adding 123
 - configuring 122
 - default 122
 - editing 124
 - removing members 96, 263
 - root
 - quotas 123
- group maps 265, 266
- groups, user 94
- GUI
 - using Web Administrator 4

H

- hard limits 122
- hardware
 - serial number 338
- HBA cards 323, 338
- head
 - defined 22
- head failover

- defined 22
- help 10
- high availability, failover 22
 - link, enabling 23
- hosts
 - adding 98, 268
 - configuring 98
 - editing 98, 268
 - naming 99
 - removing 99, 268
 - routes 166
 - trusted 98, 269
 - configuring 98
 - removing 99
- hot-spare
 - assigning 49

I

- icons, toolbar 4
- identifying port locations 25
- independent, port role 77
- indicators
 - LED status 322
- individual mirrors, viewing status 285
- initiating
 - controller recovery 24
 - failback 24
 - head recovery 24
- Internet Storage Name Service (iSNS) server 64
- IP address
 - aliasing 78
- IPMI events 303
- iSCSI 289
- iSCSI initiators 62, 288
 - configuring 62
- iSCSI LUNs 63, 290
 - thin-provisioned 63
- iSCSI target
 - configuring 60, 288
 - configuring NAS as 59
 - discovery methods 64, 291
- iSNS 291
- iSNS server 65, 291

K

- keys

- administration console 243
- Korean filename translations 59, 100

L

- LAN Manager 175

- language 36, 249
 - setting up 36

- LCD

- defined 321
 - panel 323

- LDAP

- configuring 91
 - defined 85
 - enabling 91
 - setting up 91

- LEDs

- locate 325
 - power supply status 325
 - Power/OK 219, 322
 - rear fan tray fault 324
 - rear power supply/fan tray fault 322
 - server status 322
 - service action required 322, 325
 - status indicators 322

- license 131

- limits

- hard 122
 - names
 - ADS container 88
 - container 88
 - file volume 51
 - host 99
 - scope 29
 - segment 51
 - server 16
 - soft 123

- link failover, enabling 23

- local logging
 - see logging

- Locate button/LED 322, 325

- locating drives or units 174

- locking the console 271

- logging

- audit file 161
 - event types 251
 - facilities 35
 - local 36, 250

- remote 250

- setting up 35
 - system 158, 160
 - system events 159
 - system status 285

- logical unit number

- see LUN

- lookup order

- changing 92
 - name services, verifying 89

- LUN paths

- auto-assign 20
 - dual-server system 19
 - editing 295
 - setting 20
 - single-server 18

- LUNs

- adding 47
 - creating 47
 - defined 43
 - iSCSI 63, 290
 - rebuilding 55

M

- Macintosh

- desktop DB calls 117
 - support 117

- main menu

- console 243

- man command 244

- managing

- file volume access 270
 - quotas 122
 - routes 249
 - trusted hosts 269

- mapping

- credentials 102

- memory modules 231

- menu command 243

- messages

- display language 36

- MIB files 156

- mirror buffer

- defined 133
 - threshold alerts 140

- mirror server

- configuring 135

- defined 133
- setting up 135
- mirroring
 - active server 133, 272, 273
 - breaking 141, 276, 279
 - dedicated port 135
 - defined 133
 - file volumes 274
 - mirror server 272, 273
 - port role 78
 - promoting file volume 142, 277
 - RAID 41
 - re-establishing a mirror 144, 278
 - requirements 134
 - setting up 272, 273
 - dedicated port 135
 - file volumes 136
 - warning thresholds 275
 - source server 133, 135
 - statistics 169, 287
 - status 285
 - status states 169
- monitoring
 - configuring SNMP 156
 - UPS 168
 - enabling 168

N

- name
 - container, limits 88
 - file volume 51
 - hosts 99
 - scope 29
 - segment 51
 - server 16
 - conventions 16
- name services 251, 252
 - changing lookup order 92
 - configuring 34
 - DNS 34
 - iSNS 291
 - local 34
 - NIS 34
 - NIS+ 34
 - verifying lookup order 89
- navigating 1
- navigation panel 6
- NDMP

- configuring 187
- defined 186
- setting up 186, 296
- network
 - activity, usage statistics 165
 - routes 166
 - displaying 167
- Network Data Management Protocol
 - see NDMP
- Network File System
 - see NFS
- Network Information Service
 - see NIS
- Network Information Service Plus
 - see NIS+
- network paths 249
- Network Time Protocol
 - see NTP
- NFS
 - defined 128
 - exports
 - creating 128
 - editing 129
 - removing 130
 - setting up 128
- NIC
 - configuring 25
 - defined 25
- NIC Dual-Port Cu 236
- NIC Dual-Port Fibre card 236
- NIS
 - defined 31, 86
 - setting up 31, 251
- NIS+
 - defined 32, 86
 - setting up 32
- notification levels, email notification 35
- NSSLDAP, see LDAP
- NT domain mode 175
- NTP
 - defined 68
 - setting up 69, 246
 - time synchronization 69

O

- online help 10

- options 131
 - Compliance Archiving Software 147, 194
 - API 305
 - mirroring 133
- overview
 - appliances 338–339
 - back-end storage 339
 - controller units 339
 - expansion units 339
- ownership assignment, group privilege 95

P

- parity, defined 41
- partition
 - renaming 254
- password 245
 - administrator, setting 67
- pathnames, ADS 88
- PCI card
 - replacing 236
 - slot designation 237
- PCI slot 338
- ports
 - bonding 79
 - dual-server systems 81
 - bonds 285
 - configuring 244
 - location 77
 - identifying 25
 - mirroring 78, 135
 - setting up 135
 - roles 78
 - assigning 26
 - independent 77
 - primary 77
 - private 78
 - setting dedicated port 135
- power failure
 - cluster configuration 22, 326
- power supply
 - LEDs 325
 - rear fan tray fault LED 322
 - replacing 229
 - server 325
 - status 163, 325
 - UPS 339
- power switch 321

- power users group 94
- Power/OK LED 219, 322
- powering off 218
- primary, port role 77
- private, port role 78
- privileges
 - configuring 97
 - defined 95
 - ownership assignment 95
 - root user 98
 - user groups 94, 263
- promoting a file volume 142, 277
- publishing shares in ADS 90

Q

- quotas
 - default group 122
 - default user 122
 - directory tree
 - adding 125
 - configuring 125
 - deleting 127
 - editing 126
 - enabling/disabling 261
 - group
 - adding 123
 - configuring 122
 - editing 124
 - hard limits 122
 - managing 122
 - root group 123
 - root user 123
 - soft limits 123
 - user
 - adding 123
 - configuring 122
 - deleting 124
 - editing 124

R

- RAID
 - adding 47
 - creating 47
 - error messages 302
 - levels 40
 - mirroring 41
 - parity, defined 41

- sets 40
- striping, defined 40
- RAID Controller Unit, *See* controller unit
- raidctl profile command 205
 - Solaris output 205
 - Windows output 216
- RDATE
 - setting up 69, 246, 248
 - time synchronization 69
- rear fan tray fault LED 324
- reboot 294
- rebuilding, LUN 55
- recovery
 - initiating 24
- re-establishing a mirror 144, 278
 - breaking the mirror 145
 - deleting out-of-date file volume 145, 279
 - mirroring up-to-date file volume 145, 280
- remote logging
 - see logging
 - setting up 250
- removing
 - checkpoint 181
 - directory tree quotas 127
 - group maps 266
 - group members 263
 - hosts 99, 268
 - NFS exports 130
 - shares from ADS 91
 - static shares 118, 260
 - trusted hosts 99, 269
 - user maps 265
- removing group members 96
- removing scheduled checkpoint 180
- renaming
 - checkpoint 181
 - partitions 254
- requirements
 - mirroring 134
 - server name 16
- restore timeout, defined 23
- retention period for compliance 194
- rolling upgrade 192
- root group
 - quotas 123
- root user

- privileges defined by host status 98
- quotas 123
- routes
 - defined 166
 - displaying 167
 - flags 166
 - host 166
 - managing 249

S

- SATA drives 335
- scan engine 248
- scheduled checkpoints 296
- scheduling
 - checkpoints 178
 - editing 179
- scheduling checkpoints 296
- SCSI HBA card 236
- search function
 - in help 10
- Secure clock 246
- security
 - administrator password 67
 - file volume access 270
 - locking the console 271
 - setting 111
 - static shares 117
 - unlocking the console 271
 - Windows 28
- segment
 - adding 255
 - attaching 255
 - creating 50
 - name limits 51
- segments
 - defined 45
- sending a diagnostic email 282, 341
- SendTargets request 64
- serial number 338
 - software for cluster 320
- server
 - failback 22
 - fan tray fault LED 324
 - front panel buttons 323
 - head failover 22
 - head, defined 22
 - LEDs 324

- name 16
 - conventions 16
 - power supply 325
 - power supply LEDs 325
- Server Message Block
 - see SMB
- service action required LED
 - server back 325
 - server front 322
- setting
 - administrator password 67
 - date 245
 - group quotas 122
 - language 249
 - name services lookup order 34
 - secure clock 246
 - security 111
 - time 245
 - time synchronization 246
 - time zone 70, 245
 - user quotas 122
- setting up
 - active server 135
 - ADS 29, 87, 260
 - antivirus scan 72, 248
 - autohome shares 120, 257
 - Compliance Archiving Software 194
 - controller recovery 24
 - date 70, 245
 - directory tree quotas 125
 - DNS 30, 250
 - drive letters 253
 - email notification 281
 - failback 24, 295
 - failover 294
 - FTP 172, 293
 - gateway address 27
 - group maps 265
 - group privileges 94
 - head recovery 24
 - hosts 98
 - iSCSI target 288
 - language 36
 - LDAP 91
 - local logging 250
 - mirror server 135
 - mirroring 272, 273
 - mirroring file volumes 136
 - name service 252
 - name services 34, 250
 - NDMP 186, 296
 - network adapters 25
 - NFS exports 128
 - NICs 25
 - NIS 31, 251
 - NIS+ 32
 - NTP 69, 246
 - ports 25, 244
 - mirroring 135
 - privileges 97
 - RDATE 69, 246, 248
 - remote logging 250
 - server name 16
 - shares 256
 - SMB/CIFS clients 119
 - SNMP 156, 281
 - static shares 116
 - system audit 162
 - target server 135
 - TCP/IP 244
 - time 70, 245
 - time synchronization 69, 246
 - time zone 245
 - user
 - groups 262
 - user group privileges 263
 - user maps 264
 - warning thresholds 140, 275
 - Windows security 28
 - WINS 29
- shares
 - adding 258
 - autohome
 - configuring 120
 - autohome,defined 119
 - changing 259
 - defined 114
 - deleting 260
 - publishing in ADS 90
 - removing from ADS 91
 - static
 - configuring 116
 - creating 116
 - editing 118, 259
 - removing 118
 - security 117
 - static,defined 114

- updating ADS containers 90
- sharing checkpoints 182
- shutting down 174, 293
- Simple Mail Transfer Protocol
 - see SMTP
- Simple Network Management Protocol
 - see SNMP
- SMB
 - autohome shares
 - configuring 120
 - enabling 120
 - configuring
 - clients 119
 - DOS clients 119
 - Windows clients 119
 - defined 114, 143
 - drive letter mapping 253
 - static shares 256
 - adding 116, 118, 119
 - changing 118
 - configuring 116
 - creating 116
 - defined 114
 - deleting 118
 - editing 118
 - enabling 116
 - removing 118
 - security 117
- SNMP
 - configuring 156, 281
 - defined 25, 114, 156
- soft limits 123
- software
 - File Replicator 133
 - license 131
 - mirroring 133
 - serial number 338
 - updating a cluster 192
 - updating with reboot 192
- source server 135
 - defined 133
- static shares 256
 - configuring 116
 - creating 116
 - defined 114
 - editing 118
 - removing 118

- security 117
- statistics
 - mirroring 169
- status 157, 284
 - controller information 169
 - environmental, viewing 163
 - fans 163
 - file volume usage 165
 - indicators 322
 - individual mirrors 285
 - mirror states 169
 - mirror statistics 287
 - mirroring 169
 - network activity 165
 - power supplies 163
 - system activity 165
 - temperature 163
 - UPS 168
 - voltage 164
- status LED indicator 322
- status panel 9
- storage, *See* back-end storage
- striping, defined 40
- Sun StorageTek 5220 NAS Appliance, *See* appliances
- Sun StorageTek 5320 Expansion Unit, *See* expansion units
- Sun StorageTek File Checkpoints
 - see checkpoints
- synchronizing time 69, 246
 - defined 68
- syslogd 35, 250
- SysMon, defined 300
- system 161
 - activity usage statistics 165
 - audit 161, 298
 - events 159
 - shutting down 293
 - status 322
 - status panel 9
- system log 160, 337
 - viewing 285
- system options 131
- System Overtemp LED 322

T
tape library

- attaching for backup 326
- target server
 - configuring 135
 - defined 133
- TCP/IP
 - configuring 244
- telnet 242
- temperature status 163
- thresholds
 - mirror buffer 140
 - warning 275
- time 245
 - synchronization 69
 - defined 68
 - NTP 69
 - RDATE 69
 - zone 70, 245
- time synchronization 246
 - NTP 246
 - RDATE 246, 248
- time zone 245
 - updating the database 188
- toolbar
 - icons 4
- top fan fault LED 322
- trunking
 - see bonding ports
- trusted hosts
 - adding 98, 269
 - defined 98
 - deleting 269
 - managing 269
 - removing 99
- turning the server off 174, 293
- types 292

U

- UID, defined 117
- umask 117
- uninterrupted power supply(UPS) 339
- Uninterruptible Power Supply
 - see UPS
- Unix settings
 - mapping 108, 109, 110
 - name service lookup order 34
- unlocking console 271

- updating
 - ADS share containers 90
 - software 192
 - software on cluster 192
- upgrading firmware 195, 196, 199, 204
- UPS
 - defined 167
 - enabling monitoring 168
 - error messages 300
 - monitoring 168
- usage statistics
 - file volumes 165
 - network activity 165
 - system activity 165
- USB-to-Serial cable 339
- user
 - quotas
 - adding 123
 - configuring 122
 - default 122
 - deleting 124
 - editing 124
 - for root 123
- user and group credentials, mapping 102
- user groups 262
 - adding 262
 - adding members 262
 - defined 94
 - privileges 94, 263
 - removing members 263
- user maps 264, 265

V

- variations, configuration wizard 11
- verify
 - DNS configuration 89
 - name service lookup order 89
- viewing
 - activity monitor 284
 - checkpoint analysis 285
 - controller information 169
 - environmental status 163
 - fan status 163
 - file volume usage 165
 - individual mirror status 285
 - mirror statistics 169, 287
 - network activity 165

- network routes 167
- port bonds 285
- power supply status 163
- status 157
- system activity 165
- system log 158, 160, 285
- temperature status 163
- voltage status 164
- viewing system log 158
- voltage status 164
- volume 254, 256
 - mirroring 274

- files 306, 309
- mandatory enforcement restrictions 148
- metadata 311

W

- warning thresholds 140
- Web Administrator 1, 4
 - content panel 8
 - help 10
 - navigation panel 6
 - status panel 9
 - toolbar 4

Windows

- autohome shares, defined 119
- configuring SMB/CIFS 119
- domain
 - enabling 28
- mapping credentials 108
- security models 28
- static shares, defined 114
- workgroup 28
 - file directory security 111
 - security 117

WINS

- defined 86
- setting up 29

wizard

- configuration 11
- starting 12
- variations 11

workgroup

- security 28

Workgroup mode 175

WORM 147

- administrative lock-down 307
- advisory compliance restrictions 149
- file behavior 310
- file retention 307, 311