

IBM TotalStorage NAS Gateway 500



# Administrator's Guide

**Read before using**

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

**Note**

Before using this information and the product it supports, be sure to read the general information in Appendix F, "Notices," on page 313.

**Second Edition (August 2004)**

This edition applies to the IBM TotalStorage NAS Gateway 500, Version 1.1.0 and to all subsequent releases and modifications until otherwise indicated in new editions. This second edition has been updated for Version 1.1.1 of the NAS System Software.

Order publications through your IBM representative or the IBM branch office servicing your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for reader's comments is provided at the back of this publication. If the form has been removed, you can address your comments to:

International Business Machines Corporation  
Design & Information Development  
Department CGFA

PO Box 12195  
Research Triangle Park, NC 27709-9990  
U.S.A.

You can also submit comments on the Web at [www.ibm.com/servers/storage/support](http://www.ibm.com/servers/storage/support).

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2004. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Figures</b> . . . . .	xiii
<b>Tables</b> . . . . .	xv
<b>About this manual.</b> . . . . .	xvii
Who should read this manual . . . . .	xvii
Summary of changes . . . . .	xvii
New information . . . . .	xvii
Modified information. . . . .	xvii
Publications. . . . .	xvii
NAS Gateway 500 publications by task . . . . .	xviii
Hardcopy publications shipped with the NAS Gateway 500 . . . . .	xix
Softcopy publications . . . . .	xix
Translated publications . . . . .	xx
Related publications . . . . .	xx
Additional information . . . . .	xxi
Notices and highlighting . . . . .	xxi
Case sensitivity . . . . .	xxi
Accessibility. . . . .	xxii
Web sites . . . . .	xxii

---

## Part 1. Welcome to the NAS Gateway 500 . . . . . 1

<b>Chapter 1. Introduction</b> . . . . .	3
Worksheets for initial configuration . . . . .	4
Optional software features . . . . .	4
Clustering . . . . .	4
Remote Mirroring . . . . .	4
Common Internet File System . . . . .	4
User definitions . . . . .	5
Root user . . . . .	5
NAS administrators . . . . .	6
File access users . . . . .	6
External disk SAN storage . . . . .	7
<b>Chapter 2. NAS administrator's installation checklist</b> . . . . .	9

---

## Part 2. Initial configuration . . . . . 11

<b>Chapter 3. Getting started</b> . . . . .	13
Overview . . . . .	13
Powering on the NAS Gateway 500 for the first time . . . . .	13
Special considerations . . . . .	14
Accepting the license agreement . . . . .	14
Installing the Web-based System Manager Remote Client . . . . .	15
<b>Chapter 4. Starting the WebSM Remote Client</b> . . . . .	19
<b>Chapter 5. Using the Initial Configuration Wizard</b> . . . . .	21
Prerequisites. . . . .	21
Individual wizards within the Initial Configuration Wizard. . . . .	21

<b>Chapter 6. Using the Feature Selection Wizard</b>	25
<b>Chapter 7. Using the Remote Mirroring Wizard</b>	27
Step 1 (from the remote site)	28
Step 2 (from the local site)	29
<b>Chapter 8. Using the General Setup Wizard</b>	33
<b>Chapter 9. Using the Network Configuration Wizard</b>	41
<b>Chapter 10. Using the Cluster Wizard</b>	43
<b>Chapter 11. Using the Static Routes Wizard</b>	51
<b>Chapter 12. Using the CIFS Wizard</b>	53
<b>Chapter 13. Using the Volume Wizard</b>	59
<b>Chapter 14. Using the Link Aggregation Wizard</b>	67
<b>Chapter 15. Running wizards after initial configuration</b>	71
Feature Management Wizard	72
Remote Mirroring Wizard	72
Link Aggregation Wizard	72
Static Routes Wizard	72
Cluster Wizard	72
CIFS Wizard	72
Volume Wizard	73
NAS Administrator Wizard	73
File Access User Wizard	73
<hr/>	
<b>Part 3. User interfaces</b>	<b>75</b>
<b>Chapter 16. Command line interface</b>	77
<b>Chapter 17. Using System Management Interface Tool</b>	79
<b>Chapter 18. Using WebSM after initial configuration</b>	83
<hr/>	
<b>Part 4. Managing the NAS Gateway 500</b>	<b>87</b>
<b>Chapter 19. NAS administrator common tasks</b>	89
Creating users	89
Creating NAS volumes	89
Protecting your system and data	90
<b>Chapter 20. Managing administrators</b>	91
Tasks used to manage administrators	91
Adding a new administrator	91
Changing an administrator's password	91
Showing the characteristics of an administrator	92
List of all the administrators	92
<b>Chapter 21. Managing applications</b>	93
Using Tivoli Storage Manager (TSM)	93

Configuring the TSM client . . . . .	93
Backup . . . . .	94
Restore . . . . .	94
Configuring the TSM storage agent . . . . .	95
Starting and stopping the TSM storage agent. . . . .	95
Showing or changing the boot state of the TSM storage agent . . . . .	96
Using Tivoli Storage Area Network Manager (TSANM) . . . . .	96
Configuring Tivoli SAN Manager agent . . . . .	96
Setting the password for the Tivoli SAN Manager agent . . . . .	97
Starting and stopping the Tivoli SAN Manager agent . . . . .	97
Showing or changing the boot state of the Tivoli SAN Manager agent. . . . .	97
Using Tivoli Storage Resource Manager (TSRM) . . . . .	98
Establishing quotas with TSRM . . . . .	98
Configuring the TSRM agent . . . . .	98
Starting and stopping TSRM agent . . . . .	98
Showing or changing the boot state of the TSRM agent . . . . .	99
Using Simple Network Management Protocol (SNMP) . . . . .	99
Getting SNMP information . . . . .	99
Setting SNMP information . . . . .	100
Dumping SNMP information. . . . .	100
Starting SNMP . . . . .	100
Stopping SNMP . . . . .	100
<b>Chapter 22. Managing client access . . . . .</b>	<b>101</b>
Local file access users . . . . .	101
Adding a local file access user . . . . .	101
Changing a local file access user's password . . . . .	102
Changing or showing characteristics of a local file access user. . . . .	102
Removing a local file access user . . . . .	102
Listing local file access users . . . . .	103
Setting or changing a CIFS user's password . . . . .	103
Adding a group . . . . .	103
Changing or showing characteristics of a group . . . . .	103
Removing a group . . . . .	103
Listing all groups. . . . .	104
Directory Services . . . . .	104
Configuring the NAS Gateway 500 as a NIS client . . . . .	105
Changing or showing characteristics of the client configuration . . . . .	105
Changing the NIS domain name of this host . . . . .	106
Removing NIS client configuration . . . . .	106
Initializing the system for a NIS+ client. . . . .	106
Configuring the NAS Gateway 500 as a NIS+ client . . . . .	106
Removing NIS+ client configuration . . . . .	107
NIS+ credential administration . . . . .	107
Configuring the NAS Gateway 500 as an LDAP client . . . . .	107
Removing LDAP client configuration . . . . .	108
<b>Chapter 23. Managing clustered systems . . . . .</b>	<b>109</b>
Tasks used to manage clusters . . . . .	109
Enabling the cluster. . . . .	110
Disabling the cluster . . . . .	110
Verifying clusters. . . . .	110
Synchronizing the cluster. . . . .	111
Deleting the cluster . . . . .	111
Showing cluster server state . . . . .	111
Enabling a server in the cluster . . . . .	112

Disabling a server in cluster . . . . .	112
Moving cluster service to another adapter . . . . .	113
Showing volumes being served . . . . .	113
Relocating volumes . . . . .	113
Enabling a volume in the cluster . . . . .	114
Disabling a volume in the cluster . . . . .	114
Enabling a resource group in the cluster . . . . .	115
Disabling a resource group in the cluster . . . . .	115
Viewing the cluster log. . . . .	115
Displaying information about cluster interfaces . . . . .	116
Modifying the cluster . . . . .	116
Adding a GeoPrimary network . . . . .	116
Deleting a GeoPrimary network . . . . .	116
Changing a host name in the geographic cluster . . . . .	117
Modifying a host's mirroring settings. . . . .	117
Adding another host in the geographic cluster . . . . .	117
Deleting a host in the geographic cluster . . . . .	118
<b>Chapter 24. Managing devices . . . . .</b>	<b>119</b>
Tasks used to manage devices . . . . .	119
Configuring devices . . . . .	119
Unconfiguring devices . . . . .	120
Displaying configured disks and attributes . . . . .	120
Displaying the size of a local disk . . . . .	121
Displaying installed devices and attributes . . . . .	121
Displaying additional device-specific information . . . . .	121
Removing volume information from a local physical disk . . . . .	122
Displaying the size of a remote disk. . . . .	122
Removing volume information from a remote physical disk . . . . .	123
Creating a link aggregation device . . . . .	123
Listing link aggregation devices . . . . .	123
Changing a link aggregation device . . . . .	124
Removing a link aggregation device. . . . .	124
<b>Chapter 25. Managing file serving . . . . .</b>	<b>125</b>
FTP . . . . .	125
Creating and managing FTP users . . . . .	125
Creating an anonymous FTP login . . . . .	125
Creating or enabling an anonymous FTP login user . . . . .	125
HTTP . . . . .	126
Configuring the HTTP server . . . . .	126
Managing HTTP users. . . . .	127
Creating HTTP file shares . . . . .	128
Starting, restarting and stopping the HTTP serve daemon . . . . .	128
Starting, restarting, and stopping the HTTP administration server daemon . . . . .	129
Displaying HTTP server configuration information. . . . .	129
Displaying HTTP server logs . . . . .	130
Network File System . . . . .	130
Starting Network File System . . . . .	131
Stopping Network File System. . . . .	131
Changing Network File System characteristics . . . . .	131
Displaying currently exported volumes . . . . .	132
Adding a volume to the export list . . . . .	132
Exporting and recovering snapshot data . . . . .	133
Exporting all volumes . . . . .	134
Exporting a specific volume from the export list . . . . .	134

Changing or showing attributes of an exported directory . . . . .	134
Unexporting and removing a volume from the export list . . . . .	135
Unexporting all volumes . . . . .	135
Unexporting a specific volume . . . . .	135
Mounting a volume from an AIX client . . . . .	136
Displaying remotely mounted filesystems . . . . .	136
Starting PC NFS . . . . .	136
Stopping PC NFS . . . . .	137
Common Internet File System . . . . .	137
CIFS concepts . . . . .	138
Starting the CIFS server . . . . .	139
Stopping the CIFS server . . . . .	139
CIFS server status . . . . .	139
CIFS server statistics . . . . .	139
CIFS basic setup . . . . .	140
CIFS authentication . . . . .	141
CIFS resource limits . . . . .	142
CIFS fileserver characteristics . . . . .	142
Listing all currently available CIFS Shares . . . . .	143
Creating a CIFS share . . . . .	143
Changing attributes of a CIFS share . . . . .	144
Removing a CIFS share . . . . .	144
Listing all CIFS users . . . . .	144
Mapping a Windows user to a NAS file access user . . . . .	145
Creating a CIFS user . . . . .	145
Changing a CIFS user . . . . .	146
Changing a CIFS user's password . . . . .	146
Removing a CIFS user . . . . .	146
NetBIOS Name Server . . . . .	147
Listing names in the NetBIOS Name Table . . . . .	147
Adding a NetBIOS name . . . . .	147
Deleting a NetBIOS name . . . . .	147
Deleting a NetBIOS name by address and by name . . . . .	147
Backing up a NetBIOS Name table . . . . .	148
Restoring a NetBIOS Name table . . . . .	148
<b>Chapter 26. Managing networking . . . . .</b>	<b>149</b>
Tasks used to manage networking . . . . .	149
Listing Network Adapters and Interfaces . . . . .	149
Configuring network adapters using TCP/IP . . . . .	150
Obtaining network interface statistics . . . . .	150
Configuring static routes . . . . .	151
Removing static routes . . . . .	151
Listing static routes . . . . .	151
<b>Chapter 27. Managing security . . . . .</b>	<b>153</b>
Tasks used to manage NFS and NIS security . . . . .	153
Starting the keysevr daemon . . . . .	153
Stopping the keysevr daemon . . . . .	154
Adding or changing a user's key . . . . .	154
Decrypting and storing a secret key . . . . .	154
Deleting a stored secret key . . . . .	154
Changing encryption key . . . . .	155
<b>Chapter 28. Managing the system . . . . .</b>	<b>157</b>
Backup and recovery of the system . . . . .	157

Backup configuration files . . . . .	157
Restore configuration files . . . . .	157
Boot and shutdown . . . . .	157
Shutdown the system . . . . .	158
Changing reboot options . . . . .	158
Setting the date and time . . . . .	158
Changing and showing date and time . . . . .	159
Changing the time zone . . . . .	159
Using the ntpq command. . . . .	160
Using the ntpdate command . . . . .	160
Problem determination . . . . .	160
How to access diagnostic functions using NAS SMIT . . . . .	161
Changing dump options . . . . .	161
Gathering debugging data . . . . .	161
Hardware diagnostics . . . . .	161
Tracing . . . . .	162
System information . . . . .	162
Displaying performance information . . . . .	162
Displaying network information . . . . .	163
<b>Chapter 29. Managing NAS volumes, Remote Mirrored systems, and snapshots . . . . .</b>	<b>165</b>
Managing NAS volumes . . . . .	165
Configuring physical volumes . . . . .	166
Configuring NAS volumes . . . . .	166
Creating a NAS volume . . . . .	166
Changing a NAS volume . . . . .	167
Deleting a NAS volume . . . . .	167
Defragmenting a NAS volume . . . . .	168
Exporting a NAS volume . . . . .	168
Importing a NAS volume . . . . .	169
Extending the size of a NAS volume . . . . .	169
Copying a NAS volume . . . . .	169
Replacing a disk within a NAS volume. . . . .	170
Mounting a NAS volume . . . . .	170
Unmounting a NAS volume . . . . .	170
Creating a mirror of a local NAS volume . . . . .	171
Unmirroring a local NAS volume . . . . .	171
Synchronizing a NAS volume . . . . .	171
Listing NAS volumes in a system. . . . .	172
Viewing NAS volume statistics. . . . .	172
Creating a remotely mirrored NAS volume . . . . .	173
Listing remotely mirrored NAS volumes . . . . .	173
Deleting a remotely mirrored NAS volume . . . . .	173
Extending the size of a remotely mirrored NAS volume. . . . .	174
Replacing a disk within a remotely mirrored NAS volume . . . . .	174
Viewing I/O statistics for a remotely mirrored NAS volume . . . . .	175
Clearing NAS information from a remote disk . . . . .	175
Managing Remote Mirrored systems . . . . .	175
Starting a mirror . . . . .	175
Stopping a mirror . . . . .	176
Listing mirrors. . . . .	176
Viewing mirror log files . . . . .	176
Taking mirror snapshots . . . . .	177
Listing mirror snapshots . . . . .	177
Restoring mirrors from a snapshot . . . . .	178



Managing snapshots . . . . .	178
Creating a snapshot . . . . .	178
Deleting a snapshot . . . . .	179
Renaming a snapshot . . . . .	179
Rolling back a snapshot . . . . .	180
Showing all current snapshots . . . . .	180
Configuring a snapshot schedule . . . . .	181
Managing a snapshot schedule . . . . .	182
Showing a snapshot schedule . . . . .	182
Snapshot Link Management . . . . .	183

---

**Part 5. Advanced management topics . . . . . 185**

<b>Chapter 30. System backup and recovery . . . . .</b>	<b>187</b>
Save or restore hardware management policies . . . . .	187
System recovery using mksysb . . . . .	187
Creating a system backup . . . . .	188
Using NIM . . . . .	188
Backing up to tape media or a file . . . . .	189
Installing a system backup using NIM . . . . .	190
Installing a system backup using a tape device . . . . .	192
Using the System Software Recovery CD-ROM . . . . .	193
<b>Chapter 31. Call home . . . . .</b>	<b>195</b>
Electronic Service Agent introduction . . . . .	195
How the Electronic Service Agent works . . . . .	197
Service Agent security . . . . .	201
Electronic Service Agent prerequisites . . . . .	202
Installing the Electronic Service Agent . . . . .	205
Installing Electronic Service Agent from SMIT . . . . .	205
Installing Electronic Service Agent from a command line . . . . .	206
What to do if the Electronic Service Agent installation fails . . . . .	206
Installing Electronic Service Agent client code . . . . .	208
Removing the Electronic Service Agent . . . . .	209
Uninstalling Electronic Service Agent on the monitored machine . . . . .	209
Initial start of Electronic Service Agent processes . . . . .	210
Step 1: Start Connection Manager . . . . .	211
Step 2: Start the Electronic Service Agent gateway . . . . .	211
Step 3: Start the Electronic Service Agent client . . . . .	212
Configuring the Electronic Service Agent . . . . .	212
Navigating the configuration panels . . . . .	212
Accessing the basic configuration interface . . . . .	215
Performing the basic Electronic Service Agent configuration . . . . .	216
Configuration tasks . . . . .	221
Configuration property parameter details . . . . .	227
<b>Chapter 32. Inventory Scout . . . . .</b>	<b>239</b>
<b>Chapter 33. Uninterruptible power supply . . . . .</b>	<b>241</b>
Configuring a UPS on the NAS Gateway 500 . . . . .	241
<b>Chapter 34. System upgrades and configuration changes . . . . .</b>	<b>243</b>
Adding new hardware . . . . .	243
Adding a network adapter . . . . .	243
Adding a Fibre Channel HBA . . . . .	243
Adding Remote Mirroring . . . . .	244

Adding clustering . . . . .	244
Before you begin. . . . .	244
Upgrading the system . . . . .	245
Software system upgrades . . . . .	246
Installation and Packaging of Updates . . . . .	246
Types of Update Packages . . . . .	247
Software update practices . . . . .	247
System firmware updates . . . . .	248
General information on system firmware updates . . . . .	248
Determining the level of firmware on the system . . . . .	248
Updating the firmware . . . . .	248
Using the service processor menu method . . . . .	249
Using the CLI method . . . . .	250
Archiving the update files . . . . .	250
<b>Chapter 35. Miscellaneous administration tasks . . . . .</b>	<b>251</b>
How to change SNMP V3 for single node . . . . .	251

---

**Part 6. Appendixes . . . . . 253**

<b>Appendix A. Modem configurations . . . . .</b>	<b>255</b>
Modem setup . . . . .	255
Configuring the 7852-400 Modem . . . . .	256
Configuring the 7857-017 or 7858-336 Modem. . . . .	256
<b>Appendix B. Command shortcuts using SMIT fastpath and WebSM . . . . .</b>	<b>259</b>
Managing administrators . . . . .	260
Managing applications (TSM, TSANM, TSRM, SNMP) . . . . .	261
Managing client access . . . . .	265
Managing local file access users and groups . . . . .	265
Directories . . . . .	267
Managing clustering . . . . .	271
Managing devices . . . . .	273
Managing file serving . . . . .	275
FTP command SMIT fastpaths and WebSM access . . . . .	275
HTTP command SMIT fastpaths and WebSM access . . . . .	275
NFS command SMIT fastpaths and WebSM access . . . . .	276
CIFS command SMIT fastpaths and WebSM access . . . . .	279
Managing the network. . . . .	281
Managing security . . . . .	284
Secure NFS command SMIT fastpaths and WebSM access . . . . .	284
Managing the system . . . . .	285
Backup and recovery SMIT fastpaths and WebSM access . . . . .	285
Boot and shutdown SMIT fastpaths and WebSM access . . . . .	285
Date and time SMIT fastpaths and WebSM access . . . . .	285
Problem determination SMIT fastpaths and WebSM access . . . . .	286
System information command SMIT fastpaths and WebSM access . . . . .	287
Managing volumes, Remote Mirroring, and snapshots . . . . .	289
Managing local volumes . . . . .	289
Managing remotely mirrored volumes . . . . .	291
Remote Mirroring SMIT fastpaths and WebSM access . . . . .	292
Snapshot SMIT fastpaths and WebSM access . . . . .	293
<b>Appendix C. Remote Mirroring problem determination . . . . .</b>	<b>295</b>
Site failure . . . . .	295
Handling site failures . . . . .	295

Site isolation . . . . .	296
Handling site isolation . . . . .	296
Node failure . . . . .	297
Disk failure . . . . .	297
Data divergence . . . . .	297
GeoMirror state map devices . . . . .	297
Viewing state map device information (root only) . . . . .	298
Saving state maps in map files (root only) . . . . .	298
Updating a state map device (root only) . . . . .	298
Checking and unifying state maps . . . . .	299
Previewing a unified state map . . . . .	300
Unifying state maps. . . . .	301
Site recovery after catastrophic failure . . . . .	301
<b>Appendix D. Cluster snapshot configuration . . . . .</b>	<b>303</b>
Adding a cluster snapshot . . . . .	303
Changing and showing a cluster snapshot . . . . .	304
Removing a cluster snapshot . . . . .	304
Applying a cluster snapshot. . . . .	304
Configuring a custom snapshot method . . . . .	305
Adding a custom snapshot method . . . . .	306
Changing or showing a custom snapshot method. . . . .	306
Removing a custom snapshot method . . . . .	306
<b>Appendix E. Hardware installation and service updates . . . . .</b>	<b>309</b>
Stopping the system . . . . .	309
Restarting the system . . . . .	310
Installing the OS mirroring option . . . . .	311
<b>Appendix F. Notices . . . . .</b>	<b>313</b>
Trademarks. . . . .	314
<b>Glossary . . . . .</b>	<b>315</b>
Glossary of terms . . . . .	315
<b>Index . . . . .</b>	<b>327</b>



---

## Figures

1. Remote Client Install Image Download panel . . . . .	16
2. Web-based System Manager Remote Client Log On panel . . . . .	20
3. Feature Selection panel . . . . .	25
4. Select your site . . . . .	27
5. Configure Remote Mirroring Network Ethernet Port . . . . .	28
6. Site Topology Selection . . . . .	29
7. Local Site Mirroring Network for two nodes . . . . .	30
8. Remote Site Mirroring Network for two nodes . . . . .	31
9. Set Date and Time panel . . . . .	33
10. Set root password panel . . . . .	34
11. Add or Delete NAS administrators panel . . . . .	35
12. List of Directory Services panel . . . . .	36
13. NIS Client configuration panel . . . . .	37
14. File access users panel . . . . .	38
15. Network configuration panel . . . . .	41
16. Static or dynamic IP address selection panel . . . . .	42
17. Cluster Setup . . . . .	43
18. Cluster for node with Remote Mirroring. . . . .	44
19. Cluster for node without Remote Mirroring . . . . .	45
20. Synchronize cluster . . . . .	47
21. Network configuration 1 . . . . .	48
22. Network configuration 2 . . . . .	49
23. Configure static routes . . . . .	51
24. Static route created . . . . .	52
25. Local CIFS Server . . . . .	54
26. Windows Internet Name Service . . . . .	55
27. CIFS User Authentication panel . . . . .	56
28. CIFS Local users panel . . . . .	56
29. Confirm CIFS settings panel . . . . .	57
30. Select a node panel. . . . .	60
31. Volume selection panel . . . . .	61
32. Volume configuration panel . . . . .	62
33. Remote volume configuration panel . . . . .	63
34. NAS volume creation confirmation panel . . . . .	64
35. NAS Volume Creation Complete panel . . . . .	65
36. Congratulations panel . . . . .	66
37. Select network interfaces . . . . .	67
38. Set link aggregation options . . . . .	68
39. Link aggregation complete . . . . .	70
40. Web-based System Manager panel . . . . .	71
41. NAS System Management panel . . . . .	79
42. WebSM navigation and contents panels . . . . .	84
43. Example: Problem Determination panel . . . . .	161
44. Example: System performance information panel . . . . .	163
45. Example: Show Network Statistics panel . . . . .	164
46. NAS Gateway 500 Electronic Service Agent monitored network and how it relates to IBM . . . . .	197
47. Typical NAS Gateway 500 Electronic Service Agent network . . . . .	199
48. Software install panel. . . . .	206
49. Welcome screen . . . . .	216
50. Basic Electronic Service Agent Configuration wizard - Updating network data . . . . .	217
51. Basic Electronic Service Agent Configuration wizard - Entering updated network data . . . . .	217
52. Basic Electronic Service Agent Configuration wizard - Electronic Service Agent Gateway parameters . . . . .	218

53. Electronic Service Agent advanced panel . . . . . 222  
54. Operator panel . . . . . 311

---

## Tables

1. IBM TotalStorage NAS Gateway 500 information library as it supports common user tasks	xviii
2. NAS administrator's installation checklist	9
3. SMIT menu fastpaths	80
4. HTTP configuration worksheet	126
5. System backup methods	188
6. Managed systems information	204
7. Required parameters and fields for the ASCII interface	216
8. Network properties	228
9. Gateway properties	229
10. Call Controller properties	231
11. Connection Manager properties	232
12. Dialer parameters	233
13. Register parameters	235
14. Connect parameters	235
15. CallLog parameters	235
16. E-mail alert template	236
17. Administrator SMIT fastpaths and WebSM access	260
18. TSM, TSANM, TSRM and SNMP SMIT fastpaths and WebSM access	261
19. File access user SMIT fastpaths and WebSM access	265
20. NIS SMIT fastpaths and WebSM access	267
21. NIS+ command SMIT fastpaths and WebSM access	269
22. LDAP SMIT fastpaths and WebSM access	270
23. Clustering fastpaths and WebSM access	271
24. Devices command SMIT fastpaths and WebSM access	273
25. FTP command SMIT fastpaths and WebSM access	275
26. HTTP command SMIT fastpaths and WebSM access	275
27. NFS command SMIT fastpaths and WebSM access	276
28. CIFS command SMIT fastpaths and WebSM access	279
29. Network SMIT fastpaths and WebSM access	281
30. Secure NFS command SMIT fastpaths and WebSM access	284
31. Backup and recovery SMIT fastpaths and WebSM access	285
32. Boot and shutdown SMIT fastpaths and WebSM access	285
33. Date and time SMIT fastpaths and WebSM access	285
34. Problem determination SMIT fastpaths and WebSM access	286
35. System information command SMIT fastpaths and WebSM access	287
36. Volumes command SMIT fastpaths and WebSM access	289
37. Remote Mirrored volumes command SMIT fastpaths and WebSM access	291
38. Remote Mirroring SMIT fastpaths and WebSM access	292
39. Snapshot SMIT fastpaths and WebSM access	293





---

## About this manual

This manual provides the information necessary to configure and administer the IBM® TotalStorage® NAS Gateway 500, hereafter referred to as the NAS Gateway 500. Information in this manual primarily pertains to the software associated with the NAS Gateway 500 product.

---

## Who should read this manual

This manual is for NAS Gateway 500 administrators.

The NAS Gateway 500 administrator should have experience in at least the following skills, or have access to personnel with experience in these skills:

- AIX® (NAS system software is based on AIX, so skills in AIX or UNIX would be helpful.)
- Networking and network management
- Disk management
- SAN management
- General features and capabilities of the NAS Gateway 500
- NAS clustering and remote mirroring is based on HACMP-XD, so some familiarity with HACMP-XD would be helpful
- Critical business issues (such as backup, disaster recovery, security)

---

## Summary of changes

This book contains both information previously presented in the First Edition (February 2004) of the *IBM TotalStorage NAS Gateway 500 Administrator's Guide* and major technical changes to that information.

## New information

This edition includes the following new information for Version 1.1.1:

- Link aggregation
- Remote Mirroring
- Static routes

## Modified information

This edition includes the following modified information:

- Changes to the wizards to accommodate the new functionality.
- Changes to Electronic Service Agent.
- Corrections as necessary.

---

## Publications

The following sections contain information on the publications in the NAS Gateway 500 library. The first section illustrates what manuals you can use to perform specific tasks, followed by lists of hardcopy and softcopy publications, then how to find translated publications, and the last section provides a list of related publications that might be helpful.

## NAS Gateway 500 publications by task

Table 1 shows the manuals in the NAS Gateway 500 library that contain information related to this product and that support the listed common user tasks. That is, when you are performing a specific task, you have a reference to the manual or manuals that contain the information that you need to perform that task:

Table 1. IBM TotalStorage NAS Gateway 500 information library as it supports common user tasks

Title	User tasks					
	Planning	Hardware installation	Software installation	Configuration	Operation and administration	Diagnosis, problem determination, and service
IBM TotalStorage NAS Gateway 500 Planning Guide, GA27-4335	✓	✓		✓		
IBM TotalStorage NAS Gateway 500 Hardware Installation Guide, GA27-4336	✓	✓				
IBM TotalStorage NAS Gateway 500 Quick Start Instructions, GX27-4026		✓				
IBM TotalStorage NAS Gateway 500 Administrator's Guide, SC30-4072			✓	✓	✓	
IBM TotalStorage NAS Gateway 500 Command Reference, SC30-4074			✓	✓	✓	✓
IBM TotalStorage NAS Gateway 500 CIFS File Serving Guide, SC30-4075			✓	✓	✓	
IBM TotalStorage NAS Gateway 500 Service Guide, GY27-0418		✓			✓	✓
IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide, SC30-4073			✓	✓	✓	✓
IBM TotalStorage Translated Safety Notices, GA27-4338		✓				✓

## Hardcopy publications shipped with the NAS Gateway 500

The following technical publications are shipped in hardcopy with the NAS Gateway 500. These manuals can also be found in PDF format on the NAS Gateway 500 documentation CD-ROM and at [www.ibm.com/servers/storage/support/](http://www.ibm.com/servers/storage/support/):

- *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*, GA27-4336  
This publication provides procedures for setting up, cabling, and replacing component options of the NAS Gateway 500.
- *IBM TotalStorage NAS Gateway 500 Quick Start Instructions*, GX27-4026  
This publication describes how to install the NAS Gateway 500.
- *IBM TotalStorage NAS Gateway 500 Administrator's Guide*, SC30-4072  
This publication describes how to configure the system for the NAS Gateway 500.
- *IBM TotalStorage Translated Safety Notices*, GA27-4338  
This publication contains translations of safety notices specific to IBM TotalStorage NAS products.
- Web site location for the IBM TotalStorage NAS Gateway 500 Release Notes  
This publication identifies the Web site location ([www.ibm.com/servers/storage/support/](http://www.ibm.com/servers/storage/support/)) for the NAS Gateway 500 Release Notes
- *IBM TotalStorage NAS Gateway 500 Statement of Limited Warranty*, GX27-4024  
This publication lists the warranty and translations of the warranty for the IBM TotalStorage NAS Gateway 500.

## Softcopy publications

Additional technical publications are provided in PDF format on the NAS Gateway 500 documentation CD-ROM and at [www.ibm.com/servers/storage/support/](http://www.ibm.com/servers/storage/support/).

The following publications contain additional information about the NAS Gateway 500:

- *IBM TotalStorage NAS Gateway 500 Planning Guide*, GA27-4335.  
This manual describes the requirements to consider when planning the installation of the IBM TotalStorage NAS Gateway 500.
- *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*, SC30-4073  
This manual provides information on advanced configuration of the software and problem determination for the NAS Gateway 500.
- *IBM TotalStorage NAS Gateway 500 Service Guide*, GY27-0418  
This manual provides procedures intended for service personnel to troubleshoot and repair the NAS Gateway 500.
- *IBM TotalStorage NAS Gateway 500 Command Reference*, SC30-4074  
This manual contains reference information for commands that you can use on the IBM TotalStorage NAS Gateway 500 System Software. It describes the tasks each command performs, how commands can be modified, how they handle input and output, and who can run them.
- *IBM TotalStorage NAS Gateway 500 CIFS File Serving Guide*, SC30-4075  
This manual provides information about concepts, tools, and techniques for networking NAS Gateway 500 to personal computer clients running Windows operating systems.
- *IBM TotalStorage NAS Gateway 500 Release Notes*, GX27-4027

These release notes provide product information about issues that were unresolved when the information deliverables went to production.

- *RS/6000® eServer™ pSeries® Adapters, Devices and Cable Information for Multiple Bus Systems, SA23-2778*

This manual contains information about adapters, devices, and cables for your system.

- *RS/6000 eServer pSeries Diagnostic Information for Multiple Bus Systems, SA38-0509*

This manual contains diagnostic information, service request numbers (SRNs), and failing function codes (FFCs). It is intended to supplement the service information found in the *IBM TotalStorage NAS Gateway 500 Service Guide*.

- *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*

This manual contains information about NIS and NIS+.

## Translated publications

Translated publications can be found on the following Web site:

[www.ibm.com/servers/storage/support/](http://www.ibm.com/servers/storage/support/)

## Related publications

The following manuals provide additional information about or related to the system:

- *7014 Model T00 and T42 Rack Installation and Service Guide*
- *AIX 5L Version 5.2 Commands Reference, Volume 1*
- *AIX 5L Version 5.2 Commands Reference, Volume 2*
- *AIX 5L Version 5.2 Commands Reference, Volume 3*
- *AIX 5L Version 5.2 Commands Reference, Volume 4*
- *AIX 5L Version 5.2 Commands Reference, Volume 5*
- *AIX 5L Version 5.2 Commands Reference, Volume 6*
- *AIX 5L Version 5.2 Files Reference*
- *AIX 5L Version 5.2 Glossary*
- *AIX 5L Version 5.2 Installation Guide and Reference*
- *AIX 5L Version 5.2 Operating System Installation: Getting Started*
- *AIX 5L Version 5.2 Performance Management Guide*
- *AIX 5L Version 5.2 Performance Tools Guide and Reference*
- *AIX 5L Version 5.2 Security Guide*
- *AIX 5L Version 5.2 System Management Concepts: Operating System and Devices*
- *AIX 5L Version 5.2 System Management Guide: Communications and Networks*
- *AIX 5L Version 5.2 System Management Guide: Operating System and Devices*
- *AIX 5L Version 5.2 System User's Guide: Communications and Networks*
- *AIX 5L Version 5.2 System User's Guide: Operating System and Devices*
- *AIX 5L Version 5.2 Technical Reference: Base Operating System and Extensions Volume 1*
- *AIX 5L Version 5.2 Technical Reference: Base Operating System and Extensions Volume 2*
- *AIX 5L Version 5.2 Web-based System Manager Administration Guide*
- *RS/6000 eServer pSeries ESA Guide*

---

## Additional information

The following sections describe the notices and highlighting conventions used in the NAS Gateway 500 library, and also an explanation of the importance of capitalization when entering commands.

### Notices and highlighting

The publications in the NAS Gateway 500 library contain certain notices that relate to a specific topic. The caution and danger notices also appear in the multilingual Safety Information on the documentation CD-ROM that came with the product. Each notice is numbered for easy reference to the corresponding notices in the Safety Information.

The following list also includes highlighting conventions used throughout the library.

<b>Term</b>	<b>Definition in this document</b>
Notes	These notices provide important tips, guidance, or advice.
Attention	These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
Caution	These notices indicate situations that can be potentially hazardous to you. A caution notice is placed just before descriptions of potentially hazardous procedure steps or situations.
Danger	These notices indicate situations that can be potentially lethal or extremely hazardous to you. A danger notice is placed just before descriptions of potentially lethal or extremely hazardous procedure steps or situations.
<b>Bold</b>	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
<i>Italics</i>	Identifies parameters whose actual names or values are to be supplied by the user.
Monospace	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information that you actually type.

### Case sensitivity

Everything in UNIX file systems is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the system responds that the command is “not found”. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

Case-sensitive file names on UNIX can also cause problems for personal computer clients running Windows operating systems because these operating systems normally treat file names as caseless. UNIX file names that differ only in case would be perceived as the same file name from a PC client.

## Accessibility

The softcopy version of this manual and the other publications in the NAS Gateway 500 library are accessibility-enabled for the IBM Home Page Reader.

## Web sites

This section lists the Web sites where additional technical information is found. Be sure to visit the support page that is specific to your hardware. The Web sites include FAQs, parts information, technical hints and tips, technical publications, and downloadable files, if applicable.

<b>Site</b>	<b>Description</b>
<a href="http://www.ibm.com">www.ibm.com</a>	Main IBM home page
<a href="http://www.storage.ibm.com/">www.storage.ibm.com/</a>	IBM Storage home page
<a href="http://www.ibm.com/servers/storage/support/">www.ibm.com/servers/storage/support/</a>	IBM Support home page for Storage products

---

## Part 1. Welcome to the NAS Gateway 500

The IBM® TotalStorage® NAS Gateway 500 provides network file serving. It allows client computer systems residing on a traditional Internet Protocol (IP) communications network to access disk storage residing on a fibre channel storage area network (SAN).

- Chapter 1, “Introduction,” on page 3 provides an overview of the initial configuration, user interfaces, and the day-to-day tasks necessary to manage a NAS Gateway 500.
- Chapter 2, “NAS administrator’s installation checklist,” on page 9 provides a checklist of the tasks you must perform to install and configure the NAS Gateway 500.





---

## Chapter 1. Introduction

The IBM TotalStorage NAS Gateway 500 provides network file serving. It allows client computer systems residing on a traditional IP communications network to access disk storage residing on a fibre channel storage area network (SAN). It does this by supporting network file protocols such as Network File System (NFS), Common Internet File System (CIFS), Hypertext Transmission Protocol (HTTP), and File Transfer Protocol (FTP). The NAS Gateway 500 receives file requests from client computer systems on the communications network using these network file protocols and satisfies these requests by accessing the disk storage on the SAN.

This guide contains information about these topics:

- Initial configuration of the NAS Gateway 500 including its optional software features:
  - Clustering
  - Remote Mirroring
  - Common Internet File System (CIFS)

To perform the initial configuration of the NAS Gateway 500, see Part 2, “Initial configuration,” on page 11.

- Using the NAS Gateway 500 user interfaces including:
  - Using the System Management Interface Tool (SMIT)
  - Using the Web Based System Manager (WebSM)
  - Using the command line interface (CLI)

To learn about the available user interfaces to manage the NAS Gateway 500, see Part 3, “User interfaces,” on page 75.

- Management of the NAS Gateway 500 (for day-to-day operations) including:
  - NAS administrator common tasks
  - NAS administrator management tasks including:
    - Managing administrators
    - Managing applications
    - Managing client access
    - Managing clustered systems
    - Managing remote mirrored systems
    - Managing devices
    - Managing file serving
    - Managing networking
    - Managing security
    - Managing the system
    - Managing volumes and snapshots

For information about the tasks to be performed for the day-to-day operations, see Part 4, “Managing the NAS Gateway 500,” on page 87.

- Advanced topics for the NAS Gateway 500 including:
  - System backup and recovery
  - Call home
  - Inventory scout
  - Uninterruptible power supply

- Hardware and software upgrades and configuration changes
- Miscellaneous administration tasks

For information about additional tasks, see Part 5, “Advanced management topics,” on page 185.

---

## Worksheets for initial configuration

You must complete the initial configuration of the NAS Gateway 500 before you can start using the user interfaces for additional configuration and management activities.

**Important:** The initial configuration must be accomplished using a series of wizards. These wizards are provided to simplify the initial configuration.

Worksheets provided in the *IBM TotalStorage NAS Gateway 500 Planning Guide* assist you during the initial configuration. Be sure to have these worksheets filled out and available before you start to configure the NAS Gateway 500. Your planning should also include your decisions to use the optional features of the NAS Gateway 500 and the associated additional inputs to the wizards that are needed for configuration of these optional features.

---

## Optional software features

The following are optional software features of the NAS Gateway 500:

### Clustering

The NAS Gateway 500 can be configured in a single or dual-node configuration. Clustering is an optional feature requiring two NAS Gateway 500s. Clustering provides a high level of redundancy between nodes. In the event that one node fails, the other node can assume the role of the failed node. The clustering option can be selected and configured during the initial configuration or at a later time. If you are going to configure clustering, be sure to complete the clustering worksheets that are in the *IBM TotalStorage NAS Gateway 500 Planning Guide*, GA27-4335.

### Remote Mirroring

The NAS Gateway 500 can be configured in a remote mirrored configuration. Remote Mirroring is an optional feature requiring two sites, with one or two nodes at each site. Remote Mirroring provides a high level of redundancy between sites. In the event that one site fails, the other site can assume the role of the failed site. The Remote Mirroring option can be selected and configured during the initial configuration or at a later time. If you plan to configure Remote Mirroring, be sure to complete the Remote Mirroring worksheets that are in the *IBM TotalStorage NAS Gateway 500 Planning Guide*.

### Common Internet File System

CIFS is a network file protocol that provides network file-serving capabilities for Windows clients. CIFS is an optional feature. It can be selected and configured during initial configuration or at a later time. If you are going to configure CIFS, be sure to complete the CIFS worksheets that are in the *IBM TotalStorage NAS Gateway 500 Planning Guide*.

---

## User definitions

Before you begin the initial configuration of the NAS Gateway 500, you should be familiar with the different types of users that are available in the NAS Gateway 500. There are three categories of users:

- Root user
- NAS administrators
- File access users

### Root user

**Attention:** You must log on as the root user for initial configuration. After initial configuration is completed, root access is discouraged. It can impair operation and security of the NAS Gateway 500. When you are directed to login as root, other than initial configuration, you should log in as a NAS administrator and then use the **maintshell** command to gain root authority.

The root user has no restrictions and is created as the default user on the NAS Gateway 500. The default password for this user is *password*. You must change the default password to maintain security. The primary function of the root user is to perform the initial configuration of the NAS Gateway 500. In addition, the root user can perform operations such as:

- Add or remove NAS administrators for restricted system management
- Apply software updates (PTFs, software upgrades, hardware firmware)
- Add, delete, or configure hardware system unit and adapters
- Restore the system back to factory default
- Perform advanced problem determination and diagnostics
- Configure or invoke Electronic Service Agent (Call Home) feature

The initial configuration is a root user-only function. The initial configuration must be completed before you can use the user interfaces for additional configuration and management activities.

The root user should be aware of the *restricted shell* that exists for NAS administrators to simplify management activities. See “NAS administrators” on page 6. Unless explicitly directed otherwise, all storage and NAS administration tasks and commands on the NAS Gateway 500 are to be performed by a NAS administrator user and **not** by a root user.

**Note:** The NAS administrators that you define only have access to the commands in the `/opt/nas/bin` directory and do not have visibility to commands or directories other than `/opt/nas/bin`.

### **Attention**

The root user has access to all the commands that the NAS Gateway 500 system software provides. The root user has full access to the command set for advanced or simple installation, configuration, diagnostics, management, and security-driven tasks.

Changing the preloaded software configuration of this product might not be supported and could cause unpredictable results. The following changes could adversely affect your configuration, and should **not** be done:

- Updates to preinstalled software that have not been approved by IBM
- Installing additional software products that are not included in the preloaded image
- Installing additional software products that are not included on the IBM TotalStorage NAS Gateway 500 Supplementary CD-ROM
- Creating NAS volumes outside the NAS administrator's restricted shell

For updated compatibility information, refer to the IBM Web site:

[www.ibm.com/servers/storage/support](http://www.ibm.com/servers/storage/support)

## **NAS administrators**

NAS administrators are responsible for the day-to-day administration of the NAS Gateway 500. You create one or more NAS administrators during the initial configuration of the NAS Gateway 500.

Create a NAS administrator ID during initial configuration and use the NAS administrator ID for management activities. NAS administrators operate within the boundaries of a protected shell with specialized functions that provide simplified interfaces for management of the NAS Gateway 500. This is the preferred method for managing the NAS Gateway 500.

For more information on working with NAS administrators, see Chapter 20, "Managing administrators," on page 91.

## **File access users**

File access users are users that control access to files that are being served by the NAS Gateway 500 with NFS, FTP, HTTP, and CIFS protocols. For NFS and FTP, file access users are either authenticated against the local password registry or against a directory service as determined by the directory services settings. For CIFS, authentication is configured separately and can be handled locally or remotely by an Active Directory Server (ADS) or Primary/Backup Domain Controller (PDC/BDC). For HTTP, authentication is configured with a separate utility to control access.

For more information on working with file access users, see Chapter 22, "Managing client access," on page 101.

---

## External disk SAN storage

The following back end storage disk subsystem devices are supported.

- IBM FAStT
- IBM Enterprise Storage Server® (ESS)
- IBM TotalStorage SAN Volume Controller
- IBM TotalStorage SAN Integration Server

**Notes:**

1. It is important to note that only one type of disk storage is supported at a time. You cannot use an Enterprise Storage Server, a FAStT Storage Server, or SAN Volume controller on the same gateway or on two gateways that are clustered together at the same site.
2. If you do need to mix an IBM storage device with a non-IBM storage device, or to attach non-IBM storage, then you can use the IBM TotalStorage SAN Volume Controller. See the *IBM TotalStorage Virtualization Family: San Volume Controller Planning Guide*, GA22-1052, for more information.



## Chapter 2. NAS administrator's installation checklist

Table 2. NAS administrator's installation checklist

Task	Reference
<b>Using the initial setup wizards</b>	
Confirm that worksheets are completed. <ul style="list-style-type: none"> <li><input type="checkbox"/> Cable Planning Chart</li> <li><input type="checkbox"/> Adapter configuration worksheet</li> <li><input type="checkbox"/> Remote mirroring worksheets</li> <li><input type="checkbox"/> Clustering worksheets</li> <li><input type="checkbox"/> CIFS worksheet</li> <li><input type="checkbox"/> User mapping worksheet</li> <li><input type="checkbox"/> Volume worksheet</li> <li><input type="checkbox"/> Electronic Service Agent worksheet</li> </ul>	A copy of these worksheets can be found in the Appendixes of the <i>IBM TotalStorage NAS Gateway 500 Planning Guide, GA27-4335</i> .
<input type="checkbox"/> Verify that your SAN storage is pre-configured.	See the Attention notice at the beginning of Chapter 13, "Using the Volume Wizard," on page 59.
<input type="checkbox"/> Verify that the WebSM Client workstation meets minimum requirements and that it is connected to the network.	See "Installing the Web-based System Manager Remote Client" on page 15.
<input type="checkbox"/> Confirm that all cables are connected. If clustering, verify that the cables in Feature 1001 are connected.	Refer to <i>IBM TotalStorage NAS Gateway 500 Hardware Installation Guide, GA27-4336</i> .
<input type="checkbox"/> Power on the NAS Gateway 500.	The power-on button is the white button at the top left of the display panel. Refer to <i>IBM TotalStorage NAS Gateway 500 Hardware Installation Guide, GA27-4336</i> .
<input type="checkbox"/> Enter the IP address that is displayed on the display panel on the front of the NAS Gateway 500 into a Web browser that is executing on the managing console.	See Chapter 3, "Getting started," on page 13.
<input type="checkbox"/> Accept the software license agreement.	See "Accepting the license agreement" on page 14.
<input type="checkbox"/> Install the Web-based System Manager Remote Client, if required.	See "Installing the Web-based System Manager Remote Client" on page 15.
<input type="checkbox"/> Install Subsystem Device Driver (SDD), if required.	SDD is not preinstalled on the NAS Gateway 500. It can be used for clustered or nonclustered systems. Refer to your storage documentation.
Log in to NAS Gateway 500. <ul style="list-style-type: none"> <li><input type="checkbox"/> User ID (root)</li> <li><input type="checkbox"/> Password (password)</li> </ul>	See Figure 2 on page 20.
<input type="checkbox"/> Select optional features.	See Figure 3 on page 25.
If Remote Mirroring: <ol style="list-style-type: none"> <li>1. <input type="checkbox"/> Initialize the remote node.</li> <li>2. <input type="checkbox"/> Configure Remote Mirroring from local site 25.</li> </ol>	<ol style="list-style-type: none"> <li>1. See "Step 1 (from the remote site)" on page 28.</li> <li>2. See Chapter 7, "Using the Remote Mirroring Wizard," on page 27.</li> </ol>
<input type="checkbox"/> Set date and time.	See item 1 on page 33
<input type="checkbox"/> Define root user and set password.	See item 2 on page 34.
<input type="checkbox"/> Create NAS Gateway 500 administrators and set passwords.	See item 3 on page 35.
<input type="checkbox"/> Create file access users	See item 5 on page 38.
<input type="checkbox"/> Select Directory Services.	See item 4 on page 36.

Table 2. NAS administrator's installation checklist (continued)

Task	Reference
<input type="checkbox"/> If Clustering or Remote Mirroring, configure clustering.	See Chapter 10, "Using the Cluster Wizard," on page 43.
<input type="checkbox"/> Otherwise, configure the network.	See Chapter 9, "Using the Network Configuration Wizard," on page 41.
<input type="checkbox"/> Define network static routes.	See Chapter 11, "Using the Static Routes Wizard," on page 51.
<input type="checkbox"/> If using CIFS, configure CIFS.	See Chapter 12, "Using the CIFS Wizard," on page 53.
<input type="checkbox"/> If storage is not pre-configured, then complete configuration of storage.	See Chapter 13, "Using the Volume Wizard," on page 59.
<input type="checkbox"/> Create volumes.	See "Managing NAS volumes" on page 165.
<b>Electronic Service Agent</b>	
Verify prerequisites for Electronic Service Agent:	See "Electronic Service Agent prerequisites" on page 202.
<ul style="list-style-type: none"> <li><input type="checkbox"/> Root authority</li> <li><input type="checkbox"/> Free disk space</li> <li><input type="checkbox"/> RSH DSH or FTP-capable</li> <li><input type="checkbox"/> IBM diagnostics installed</li> <li><input type="checkbox"/> Java available</li> <li><input type="checkbox"/> Serial port 2 available</li> <li><input type="checkbox"/> Modem set up and configured</li> </ul>	See Appendix A, "Modem configurations," on page 255.
<ul style="list-style-type: none"> <li><input type="checkbox"/> Telephone connected and operational</li> <li><input type="checkbox"/> PPP installed, configured and running</li> <li><input type="checkbox"/> E-mail service available</li> <li><input type="checkbox"/> Host name, machine type, model and serial number available</li> </ul>	
Complete Electronic Service Agent installation	See "Installing the Electronic Service Agent" on page 205.
<ul style="list-style-type: none"> <li><input type="checkbox"/> Install Service Agent Gateway from SMIT or CLI</li> <li><input type="checkbox"/> Configure Electronic Service Agent</li> </ul>	
<b>Service Processor</b>	
<input type="checkbox"/> Managing console attached to serial port 1	



---

## Part 2. Initial configuration

After you have completed the hardware setup for the NAS Gateway 500, as described in the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*, you must complete the software initial configuration.

This section contains the following chapters:

- Chapter 3, “Getting started,” on page 13 provides initial power-on instructions and instructions for installing the Web-based System Manager Remote Client.
- Chapter 4, “Starting the WebSM Remote Client,” on page 19 describes using the Web-based System Manager Remote Client.
- Chapter 5, “Using the Initial Configuration Wizard,” on page 21 describes using the Initial Configuration Wizard.
- Chapter 6, “Using the Feature Selection Wizard,” on page 25 allows the selection of purchased features that are optional to the NAS Gateway 500.
- Chapter 7, “Using the Remote Mirroring Wizard,” on page 27 provides information about Remote Mirroring.

**Note:** When Remote Mirroring is used, before full Initial Configuration can be performed, limited configuration must be done at the remote site to allow network communications between the sites. First, start initial configuration at the remote site; when the Remote Mirroring Wizard is reached, perform Step 1; initial configuration exits. After this remote site network configuration is completed, start initial configuration at the local site and select Step 2 at the Remote Mirroring Wizard. All remaining configuration is performed from the local site and propagated to all other nodes (local and remote).

- Chapter 8, “Using the General Setup Wizard,” on page 33 provides information about general configuration tasks, such as setting date and time, creating NAS administrators, setting the root password, indicating whether you want to use directory services (NIS), and creating file access users.
- Chapter 9, “Using the Network Configuration Wizard,” on page 41 provides information about configuring a single-node NAS Gateway 500.
- Chapter 10, “Using the Cluster Wizard,” on page 43 provides information about configuring clustering.
- Chapter 11, “Using the Static Routes Wizard,” on page 51 provides information on static routing.
- Chapter 12, “Using the CIFS Wizard,” on page 53 provides information about initially configuring file sharing.
- Chapter 13, “Using the Volume Wizard,” on page 59 provides information about creating NAS volumes on the NAS Gateway 500.
- Chapter 14, “Using the Link Aggregation Wizard,” on page 67 provides information on link aggregation.
- Chapter 15, “Running wizards after initial configuration,” on page 71 provides information about returning to the wizards after you have completed initial configuration.



---

## Chapter 3. Getting started

This chapter provides information that you use to set up initial communication and install the software necessary for the initial configuration of the NAS Gateway 500.

After you have completed the hardware setup for the NAS Gateway 500, as described in the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*, GA27-4336, you must complete the software initial configuration. Once the initial configuration process is complete, your NAS Gateway 500 is ready to serve files across the network.

**Important:** This must be accomplished using a Web browser and the wizards described in this section.

---

### Overview

This overview outlines the process of initial configuration. The process is:

1. Power on the NAS Gateway 500. If this is a clustered configuration, power on all the NAS Gateway 500s.
2. Use a Web browser to accept the license agreement.
3. Use a Web browser to download a client program that is used for both initial configuration and day-to-day management.
4. Installation of the client program.
5. If you want to use Remote Mirroring, you must execute the Initial Configuration Wizard at the remote site first to establish communication between the sites.
6. Execute the Initial Configuration Wizard on the local site.

Once these phases are complete, the NAS Gateway 500 is ready to serve files.

---

### Powering on the NAS Gateway 500 for the first time

The NAS Gateway 500 operates in a “headless” mode. A headless machine is a machine that does not have a monitor, keyboard, or mouse directly attached. Initial configuration is accomplished using a separate graphics-capable administrative machine running AIX, Linux or Windows that is connected to the NAS Gateway 500 using a network connection. The administrative machine must have the Web-based System Manager (WebSM) Remote Client installed. See “Installing the Web-based System Manager Remote Client” on page 15 for installation of the WebSM Remote Client.

The first time you power on the NAS Gateway 500, the system attempts to contact a DHCP server to get an IP address. If it does not find one, it assigns a static IP address. In either case, the IP address is displayed on the operator panel of the NAS Gateway 500. Use this IP address to perform the initial setup and configuration of the NAS Gateway 500. You should record this IP address for later use.

---

## Special considerations

1. If clustering, then one node is chosen as the *primary node*. It is used to configure both nodes in the cluster. If using remote mirroring, there is a primary node at each site. A single node gateway is its own primary node. It is this primary node's IP address that is used first (for accepting the software license agreement and "Installing the Web-based System Manager Remote Client" on page 15). When remote mirroring, the remote site's primary node is used first. After Step 1 of initial configuration completes on the remote site primary node, then you must log on to the local site primary node to complete Step 2 of initial configuration for the entire geographic cluster.
2. You must configure your external storage on the devices before you can create volumes on the NAS Gateway 500. You do this through standalone clients, using the software provided by the storage manufacturer. If you need the World Wide Port Name (WWPN) for the fibre channel host bus adapters installed in your NAS Gateway 500, open a Web browser and enter:

`http://HostAddress/NAS500GetWWN.html`

where *HostAddress* is the host name or IP address that is assigned to the NAS Gateway 500 (or, in the case of a cluster, a specific node).

The NAS Gateway 500 is capable of attaching to multiple types of disk storage devices and uses different device drivers depending on the device to which it is attached. If you are using a device that requires the usage of the Subsystem Device Driver (SDD) in a clustered environment, the process of configuring a NAS volume is slightly altered. The driver must be installed before you define any NAS volumes.

**Caution:** Do not perform any NAS volume configuration before installing the SDD. You will lose your volume configuration information if you install the SDD afterwards.

See Chapter 13, "Using the Volume Wizard," on page 59 for information about the SDD and how it changes NAS volume configuration.

---

## Accepting the license agreement

You must accept the license agreement to begin the initial configuration process. You are not able to access the WebSM Remote Client to configure the NAS Gateway 500 until you have accepted the license agreement.

To accept the NAS Gateway 500 System Software license agreement:

1. From Windows or Linux, open a frames-capable Web browser. Enter the IP address from the LCD panel on the front of the NAS Gateway 500.
2. A Web page for language selection is displayed. Make your language selection and click **Continue**. This sets the default language that is used on the NAS Gateway 500.
3. A Web page for the license agreement for the NAS Gateway 500 System Software is displayed. Read the license agreement and click **Accept**.
4. Select a different language on the license acceptance page, if desired. This changes the language used to display the license text. It does not change the default language for the NAS Gateway 500.
5. After you accept the license agreement, the default html page (index.html) on the NAS 500 Gateway is renamed to NAS500Index.html, leaving no default page. Subsequent access to the default page results in a file listing being

displayed on the Web browser. If you need to rerun the portion of the initial configuration that allows language selection of the license agreement, you must point your browser to the NAS500Index.html page.

**Note:** If you click **Decline**, a Web page appears providing a link to the license acceptance page. Failure to accept the license agreement means you will not be able to proceed with the configuration of the NAS Gateway 500.

---

## Installing the Web-based System Manager Remote Client

This section provides information about installing the software necessary for configuring the NAS Gateway 500. The WebSM Remote Client is a Java client application that allows you to perform initial configuration and administrative tasks on the NAS Gateway 500 from a graphics-capable network attached PC or AIX workstation. It is commonly referred to as *WebSM*. Installation of the WebSM Remote Client is an option provided immediately after you accept the NAS Gateway 500 System Software license agreement. You do not need to install the WebSM Remote Client when using an AIX system; it is already a part of the operating system.

The minimum requirements for the WebSM Remote Client are:

- 1 Ghz processor
- 75 MB free disk space
- 512 MB of memory

The supported operating systems are:

- Microsoft Windows NT 4.0, Windows 2000 and Windows XP
- Red Hat Linux, versions 7.2 or 7.3
- AIX (no installation necessary)

**Note:** The panels shown in this section are from a WebSM Remote Client running on a Windows machine.

To install the WebSM Remote Client:

1. Open a frames-capable Web browser from Windows or Linux (this may already be opened).
2. Accepting the license agreement displays the Remote Client Install Image Download Web page. From this page you can select the installation image that you want to download. The client workstation that you use for the initial configuration of the NAS Gateway 500 determines the image that you need to download and install. Click one of the following:
  - **Windows NT/2000/XP**
  - **Linux**

For example, if you intend to use a Windows terminal, click **Windows NT/2000/XP**. Be sure to remember the location that you choose to store the installation image during the download process. If you do not need to download the WebSM client, close the browser now.

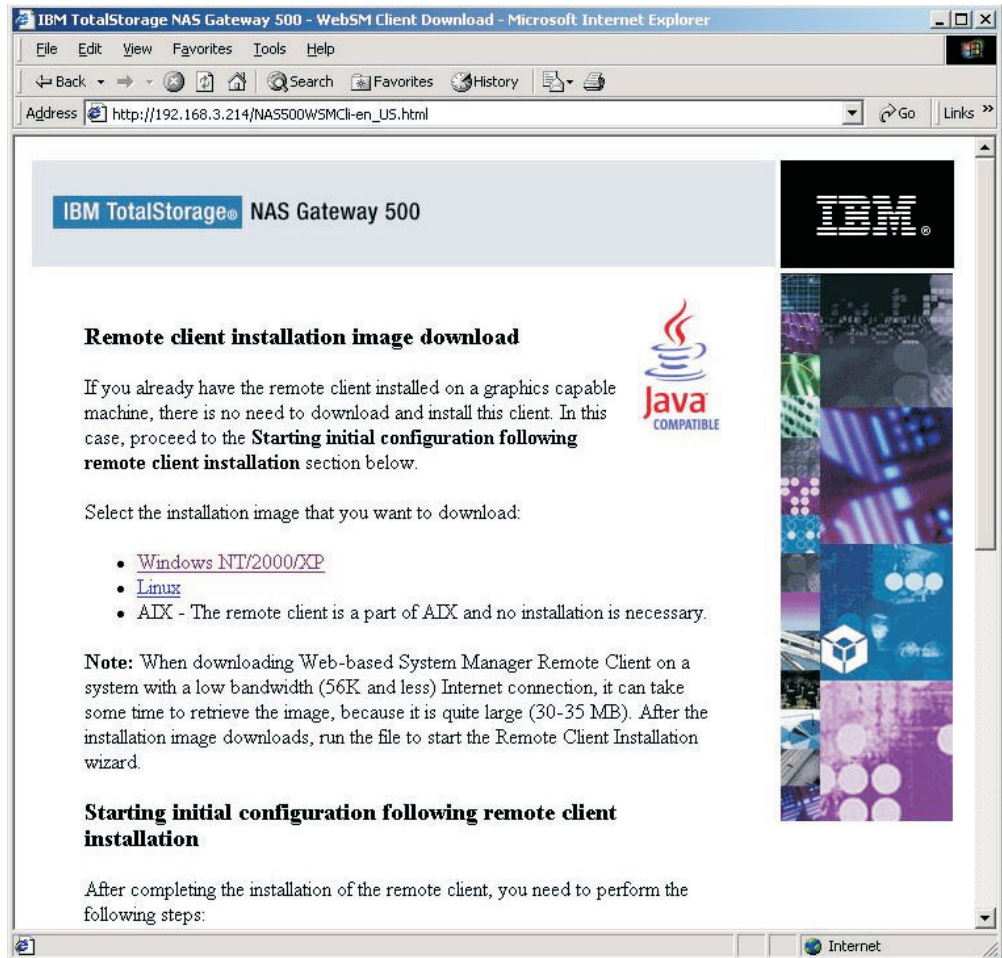


Figure 1. Remote Client Install Image Download panel

3. Once you have completed the download, you need to install the WebSM Remote Client.
  - For Windows systems, execute the file you just downloaded (setup.exe). It can be started from a Windows command prompt.
  - For Linux systems, you must first change the permissions of the downloaded file (wsmlinux.exe) to make it executable and then start it by entering **wsmlinux.exe** from a command prompt.
4. The InstallShield Wizard performs the necessary preliminary installation steps. Some popup windows are displayed during this process. The Welcome to the InstallShield Wizard for Web-based System Manager Remote Client panel is displayed when the preparation is finished. Follow the prompts to complete the installation of the WebSM Remote Client.

**Note:** If you need to install the WebSM Remote Client on additional machines, you can bring up the remote client download page again by entering the address in a Web browser.

If the desired language is English, the address is:

`http://HostAddress/NAS500WSMcli-en_US.html`

For Japanese, the address is:

[http://HostAddress/NAS500WSMcli-ja\\_JP.html](http://HostAddress/NAS500WSMcli-ja_JP.html)

*HostAddress* is the host name or IP address that is assigned to the NAS Gateway 500 or the primary node in the case of a cluster. The primary node is the node of the cluster which has been connected to the WebSM client workstation for the purpose of configuring all nodes in the cluster. All configuration is performed on the primary node and the configuration is propagated to all other nodes.





---

## Chapter 4. Starting the WebSM Remote Client

**Note:** Before beginning the software initial configuration, verify that you have connected Ethernet cables to all the Ethernet adapters to which you plan to assign an IP address. If you assign an IP address to an adapter that has no Ethernet cable, it causes connection failures in that IP address's subnet.

To begin the initial configuration process, ensure that the Web-based System Manager Remote Client installation has been completed and that you have accepted the license agreement. See "Installing the Web-based System Manager Remote Client" on page 15 for more information.

**Note:** You cannot access the WebSM Remote Client if you have not accepted the license agreement.

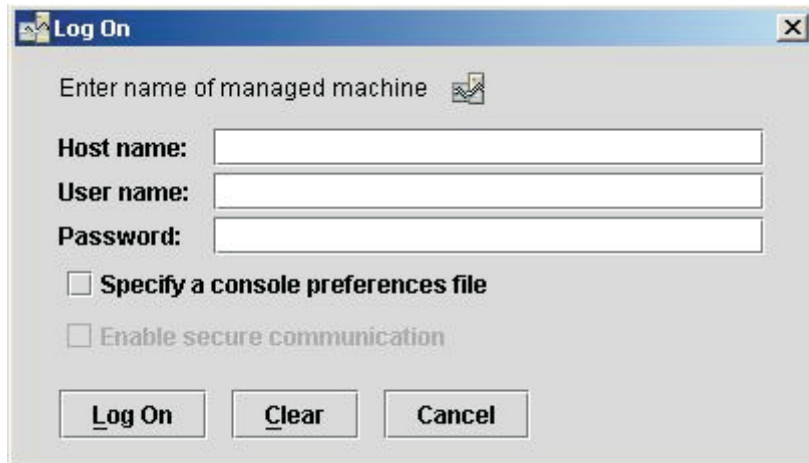
1. Start the WebSM Remote Client.

**Windows** Double click the desktop icon called Web-based System Manager Remote Client to start the client.

**Linux** Run the file called *wsm* that is in the bin directory off the directory you specified during installation of the remote client. The default installation directory is */opt/websm* and if you used the default, you would enter */opt/websm/bin/wsm* from a shell prompt.

**AIX** Enter **wsm** from a command prompt on a machine that has X-Windows capability.

2. When the Log On window appears, log on to the WebSM Remote Client by entering the following information:
  - a. Host name: Enter the IP address that was displayed on the front of the primary NAS Gateway 500 node at initial power-on.
  - b. Press the tab key and wait until communication has been established. In the message line just below the title bar, you see "Handshaking with server" while the WebSM client establishes a session with the NAS Gateway 500. Once the session has been established, this message is replaced with "Login to the management server"; at that time, proceed to step 2c.
  - c. User Name: enter **root**.
  - d. Password: enter **password**.
  - e. Click **Log On** to access the NAS Gateway 500.



*Figure 2. Web-based System Manager Remote Client Log On panel*

When the logon is completed, the WebSM main panel is displayed. Start in the right pane by clicking **Initial Configuration Wizard** to open another window containing the Initial Configuration Wizard GUIs. Continue with Chapter 5, “Using the Initial Configuration Wizard,” on page 21.

---

## Chapter 5. Using the Initial Configuration Wizard

---

### Prerequisites

Meet the following prerequisites before beginning the Initial Configuration Wizard:

#### All Configurations

Have the completed Planning Guide worksheets available.

#### Single node configurations

The NAS Gateway 500 is powered on and the operating system initialized.

#### Clustered configurations

This configuration refers to a clustered node pair at a single site.

1. Both nodes of the clustered NAS Gateway 500 must be installed in adjacent locations in the same rack. This allows the Ethernet Crossover cable and the serial null modem cable assembly to reach between all nodes.
2. You must have an Ethernet crossover cable connecting both servers through integrated Ethernet port number 2. This cable is included with the Cluster Interconnect Kit (Feature Code 1001).
3. You must have a null modem cable assembly connecting both servers using serial port 3 on both servers. This cable is included with the Cluster Interconnect Kit (Feature Code 1001).
4. Both NAS Gateway 500s must be powered on and the operating system must be initialized.

#### Remote Mirrored configurations

This configuration refers to a GeoCluster involving two sites with one to two clustered nodes at each site.

1. Determine the number of nodes at each site in your geographic cluster, and:
  - a. For sites with one cluster node ensure the prerequisites for a single node are met.
  - b. For sites with two clustered nodes verify the prerequisites for clustered configurations.
2. Ensure that at least one GeoNetwork can connect the local and remote sites (use of more than one GeoNetwork is recommended).

**Note:** At least one GeoNetwork is required for configuration to succeed.

---

### Individual wizards within the Initial Configuration Wizard

**Note:** The wizards are best viewed with a screen resolution of 1024x768. Use of other resolutions results in the truncation of some data display fields.

Single node systems, clustered systems, and Remote Mirrored systems order individual wizards differently.

#### Single node systems

A single node system has no Clustering and Remote Mirroring enabled. The wizards run in the following order:

1. Feature Selection Wizard (allows selection of CIFS File Serving)

2. General Setup Wizard (sets the date, time, root password, and so on)
3. Network Configuration Wizard (optionally runs the Link Aggregation Wizard and then configures the Ethernet ports)
4. Static Routes Wizard
5. CIFS Wizard (if CIFS was selected in the Feature Selection Wizard)
6. Volume Wizard (configures NAS volumes, sharing and snapshots)

### Clustered systems

**Note:** In clustered systems, the WebSM client workstation used for configuration attaches to a single node of the cluster that is designated as the primary node. The Initial Configuration Wizard is run on the primary node only, and the second node is configured automatically.

The wizards run in the following order:

1. Feature Selection Wizard (allows selection of CIFS File Serving and Clustering)
2. General Setup Wizard (sets the date, time, root password, and so on)
3. Cluster Wizard (optionally runs the Link Aggregation Wizard and configures IP addresses)
4. Static Routes Wizard
5. CIFS Wizard (if CIFS was selected in the Feature Selection Wizard)
6. Volume Wizard (configures NAS volumes, sharing and snapshots)

### Remote mirrored systems

**Note:** When Remote Mirroring is used, before you perform full initial configuration, you must do some limited configuration at the remote site. This allows network communication between the sites. First, start initial configuration at the remote site. Then, when the Remote Mirroring Wizard is reached, perform step 1 (see Chapter 7, “Using the Remote Mirroring Wizard,” on page 27) and initial configuration exits. After this remote site network configuration is completed, start initial configuration at the local site and select step 2 (see Chapter 7, “Using the Remote Mirroring Wizard,” on page 27) at the Remote Mirroring Wizard. All remaining configuration is performed from the local site and propagated to all other nodes (local and remote).

The wizards run in the following order:

1. Remote node — Feature Selection Wizard (allows for the selection of Remote Mirroring)
2. Remote node — Remote Mirroring Wizard (**perform Step 1**)
3. Local node — Feature Selection Wizard (allows selection of CIFS File Serving, Clustering, and Remote Mirroring)
4. Local node — Remote Mirroring Wizard (**perform Step 2**)
5. Local node — General Setup Wizard (sets the date, time, root password, and so on)
6. Local node — Cluster Wizard (optionally runs the Link Aggregation Wizard and configures IP addresses)
7. Local node — Static Routes Wizard
8. Local node — CIFS Wizard (if CIFS was selected in the Feature Selection Wizard)

9. Local node — Volume Wizard (configures NAS volumes, sharing and snapshots)

**Note:** Most wizards can be run from WebSM after initial configuration is complete. See Chapter 15, “Running wizards after initial configuration,” on page 71 for more information.



## Chapter 6. Using the Feature Selection Wizard

The Feature Selection Wizard allows you to select optional purchased features of the NAS Gateway 500. After completing initial configuration, you can return to this wizard using the WebSM interface and specify the feature you want to configure. Selecting a feature causes the appropriate configuration wizard to be executed.

1. A welcome panel appears (if you are performing initial configuration). Click **Next**.
2. Use this panel to select the optional features: Clustering, Remote Mirroring (if Clustering is chosen) and CIFS File Serving. Click the check box beside the feature to select the feature. You can select more than one feature.

**Note:** You must have a clustered system to use Remote Mirroring. This option is unavailable unless you select the clustering feature.

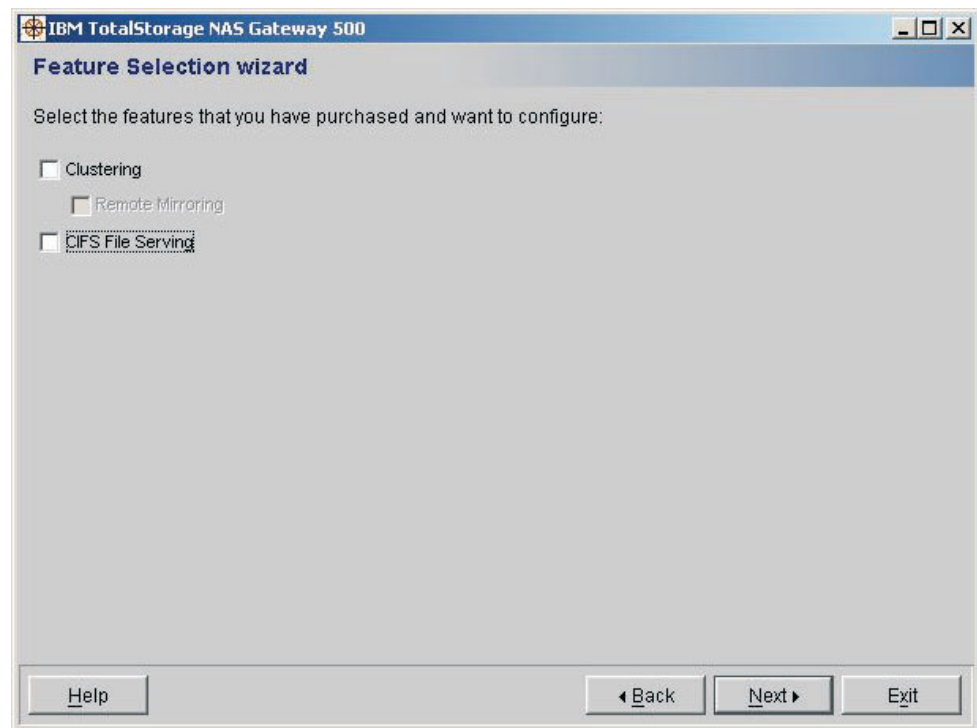


Figure 3. Feature Selection panel

If you are using remote mirroring, and this is the initial configuration at the local site (Step 2), you must select exactly the same features that you selected at the remote site during Step 1 of initial configuration.

3. Click **Next** to finish the wizard. When you click **Next**, you are automatically placed into the appropriate wizard based on the features you selected.





## Chapter 7. Using the Remote Mirroring Wizard

**Note:** When Remote Mirroring is used, before full initial configuration can be performed, some limited configuration must be done at the remote site to allow network communications between the sites.

First, start initial configuration at the remote site by attaching a WebSM client workstation to a node at the remote site; when the Remote Mirroring Wizard is reached, perform Step 1 and then initial configuration exits. At this point, close the WebSM client.

After the configuration of a communications path for the remote site is completed, start initial configuration at the primary node of the local site. The local primary node is the node selected by the WebSM client at the local site for configuration. When the Remote Mirroring Wizard prompts for a site, select Step 2. All remaining system configuration is performed from the local primary node and is propagated to all remaining nodes at both sites.

The Remote Mirroring Wizard allows you to configure Remote Mirroring. You can start it by:

- Performing initial configuration
- Running the Feature Selection Wizard (after initial configuration)
- Launching it from the WebSM maintenance tree

When the Remote Mirroring Wizard is started, you see the following panel:

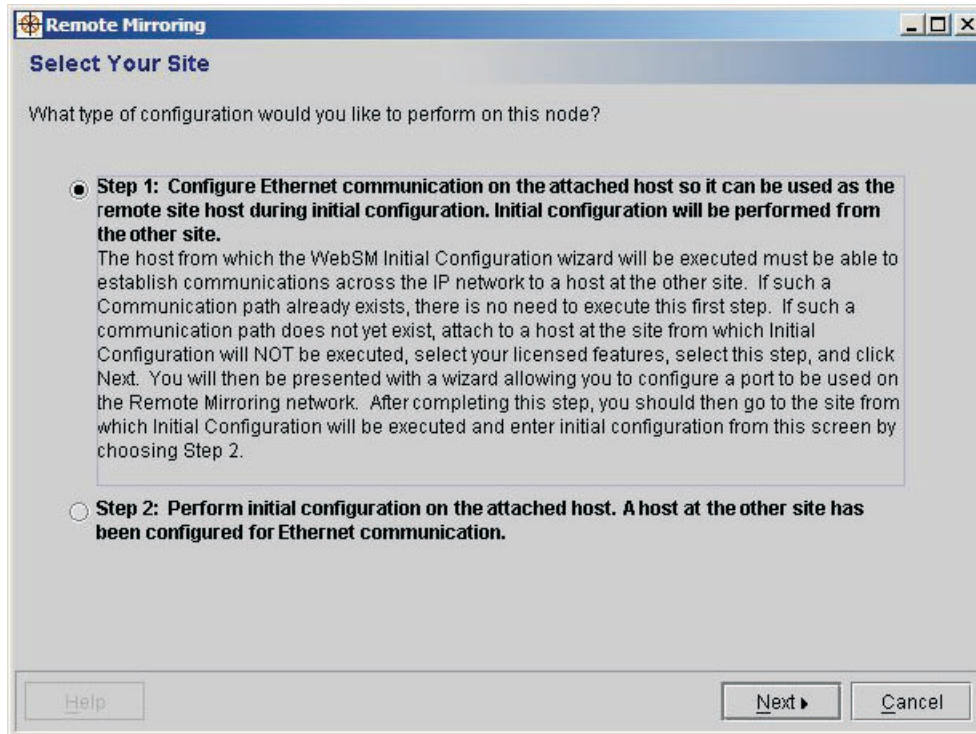


Figure 4. Select your site

You have two options in this panel:

- Step 1 (from the remote site)
- Step 2 (from the local site)

---

## Step 1 (from the remote site)

You should be logged in to the remote site primary node to configure the communication path between the remote and local nodes. Select **Step 1** and click **Next**; the following panel appears:

**Remote Mirroring**

### Configure Remote Mirroring Network Ethernet Port

Select a port and an IP address for the Remote Mirroring network on this host. If you wish to use Link Aggregation, you can aggregate ports with EtherChannel by clicking the button below.

**Card/Port:**

**IP Address:**

**Subnet Mask:**

#### Configure Static Route

If the node from which Initial Configuration will be executed is on a different subnet from the above IP address, please specify a gateway address and a destination IP address. The destination IP address is the IP to be assigned to the Remote Mirroring network on the host from which Initial Configuration will be executed.

IP Address of Gateway to Configuration Site:

IP Address of Configuration Host:

Figure 5. Configure Remote Mirroring Network Ethernet Port

1. Select a port from the drop down list.
2. Specify the IP address and subnet mask. This remote site IP address will be used in step 3 on page 29. The IP address specified should be the one that will later be assigned to the first GeoNetwork, a network dedicated to mirroring and not file serving.
3. If you want multiple ports to be used for this communications path and you have a properly configured Ethernet switch, you can use link aggregation to aggregate Ethernet ports. To do this, click **Configure Link Aggregation** (this launches the Link Aggregation Wizard; see “Link Aggregation Wizard” on page 72 for more information).

**Note:** If the remote node being configured and the local node (primary node) that will be used for configuration are on different subnets, then you must

configure a static route between the two nodes by specifying the IP address of the gateway to the local primary node, and the IP address of the local primary node.

Click **Next**. A panel appears indicating that you have completed the necessary configuration for the remote site. Click **Finish** and exit the WebSM Client. Now you should log on to the WebSM Client on the local site's primary node and restart initial configuration; this time, select **Step 2** in the Remote Mirroring Wizard to complete the configuration on all the nodes in the geographic cluster.

---

## Step 2 (from the local site)

You must already have a communications path established between the two sites and be logged in to the primary node of the local site with your WebSM client to complete initial configuration on the mirroring cluster.

1. Select **Step 2** on the Select Your Site (see Figure 4 on page 27) panel and click **Next**.
2. The Site Topology Selection panel appears:

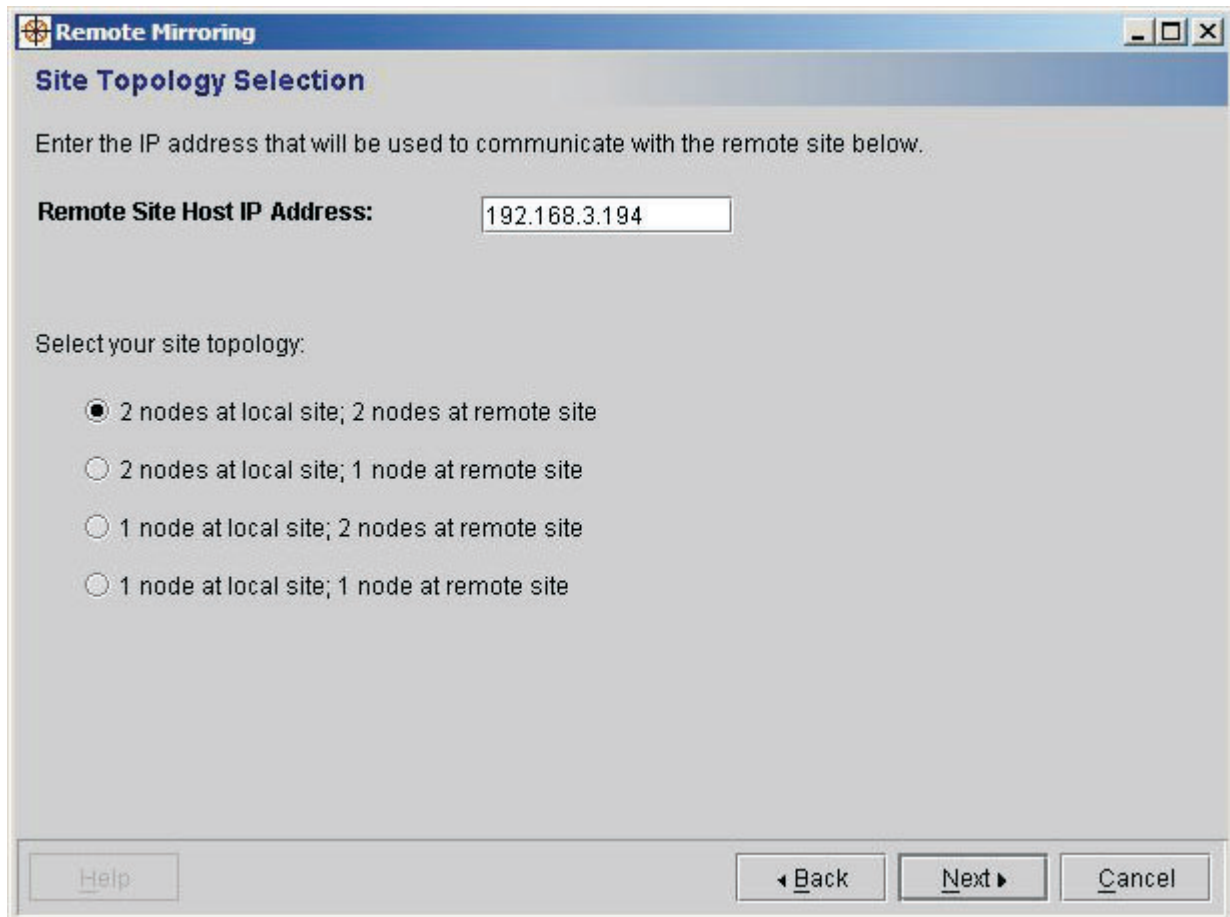


Figure 6. Site Topology Selection

3. You are then asked to enter the Remote Site Host IP Address from step 2 on "Step 1 (from the remote site)" on page 28 and select your site topology. Choices for site topology are:
  - Two nodes at local site; two nodes at remote site

- Two nodes at local site; one node at remote site
  - One node at local site; two nodes at remote site
  - One node at local site; one node at remote site
4. Click **Next** to configure your networks to be used for remote mirroring, which are called the *GeoNetworks*. You will see a panel for the local site mirroring network, followed by a panel for the remote site mirroring network. The number of nodes that display on each panel depends on the Site Topology selection for that site (either one or two).

**Remote Mirroring**

**Local Site Mirroring Network**

To configure your Ethernet adapters for link aggregation, please click the button below.

**Configure Link Aggregation**

Local Site Name: Tucson\_FVT

Subnet Mask: 255.255.255.0

Gateway to Remote Site:

Node 1 Host Name: Primary01

Card/Port: ent2 Card in slot 4 port 2 (2-Port Gigabit Ethernet-SX PCI-X Adapter)

IP Address: 192.168.3.86

Node 2 Host Name: Peer02

Card/Port: ent4 Card in slot 6 port 2 (2-Port 10/100/1000 Base-TX PCI-X Adapter)

IP Address: 192.168.3.87

Dominant Site?

Help    < Back    Next >    Cancel

Figure 7. Local Site Mirroring Network for two nodes

5. If you want to aggregate multiple Ethernet ports for increased performance and availability and you have a properly configured Ethernet switch, click **Configure Link Aggregation** to aggregate one or more ports together. This will launch the Link Aggregation Wizard as described in Chapter 14, “Using the Link Aggregation Wizard,” on page 67.
6. Enter a site name, subnet mask, and the default gateway IP address. You must use a site name ranging from one to 21 alphanumeric or underscore characters.
7. Click to select **Dominant site**, if appropriate. The dominant site is the site that will take over in case all communication is lost between sites.
- You can select either the local or remote site as the dominant site. Only one site can be dominant. For topologies with two nodes at a local site and two nodes at a remote site, or one node at a local site and one node at a remote site, when the site becomes isolated (all mirroring network connections between sites are lost) and the subordinate site determines that the dominant site is still alive, the non-dominant site takes itself down by stopping the cluster. If the cluster does not stop within two minutes, the subordinate site

shuts itself down. In the case of two nodes at one site and one node at the other, dominance does not apply; the site with the least number of nodes takes itself down.

8. Enter the information for the first node:
  - a. Node 1 Host Name.

The host name can be from one to 31 alphanumeric or underscore characters only; although you cannot begin the host name with a number. The names must be unique; if the names are longer than 24 characters, at least one of the first 24 characters must be unique.
  - b. Select the proper Adapter Card slot and port number.
  - c. Enter the IP address for this port.
9. If your site has two nodes, then enter the appropriate information for the second node.
10. Click **Next** to continue to the Remote Site Mirroring Network panel.

Remote Mirroring

### Remote Site Mirroring Network

To configure your Ethernet adapters for link aggregation, please click the button below.

[Configure Link Aggregation](#)

Remote Site Name: RTP\_PUB

Subnet Mask: 255.255.255.0

Gateway To Local Site:

Node 1 Host Name: lenny03

Card/Port: ent4 Card in slot 6 port 1 (10/100/1000 Base-TX PCI-X Adapter)

IP Address: 192.168.3.76

Node 2 Host Name: benny04

Card/Port: ent4 Card in slot 6 port 1 (10/100/1000 Base-TX PCI-X Adapter)

IP Address: 192.168.3.77

Dominant Site?

[Help](#) [More Mirroring Networks](#) [Back](#) [Next](#) [Cancel](#)

Figure 8. Remote Site Mirroring Network for two nodes

The number of fields in the Remote Site Mirroring Network panel will depend on the number of nodes at this site. Figure 8 is for a site with two nodes; if your site has only a single node, then the fields for the second node will not appear.

11. Enter the appropriate information for the Remote Site Mirroring Site just as you just did for the Local Site. If you need to configure any ports for link aggregation, you can select the **Configure Link Aggregation** button.
12. You can add additional GeoNetworks by clicking **More Mirroring Networks**, which repeats these same network screens for subsequent networks. One GeoNetwork is required, and at least two GeoNetworks are highly recommended.
13. When you are finished adding mirroring networks, click **Next** to continue to the General Setup wizard.



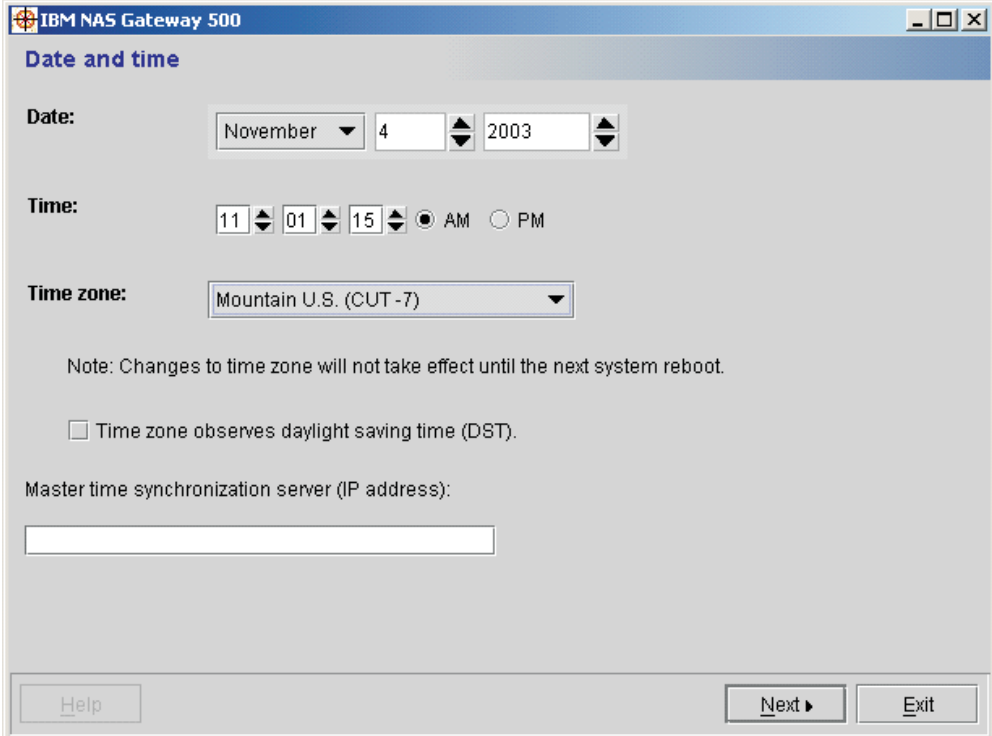
## Chapter 8. Using the General Setup Wizard

The General Setup Wizard performs the following tasks:

- Setting the date and time
- Setting the root password
- Creating and deleting NAS administrators
- Indicating whether you want to use directory services (NIS)
- Creating file access users

To use the General Setup Wizard:

1. Use the set date and time panel to set the system date and time. Use the scroll buttons to select the month, date, and year. Use the drop-down menu to select your time zone. Click to indicate if your area observes Daylight Saving Time. Enter the address of the Master Time Synchronization Server IP address (optional). Click **Next**.



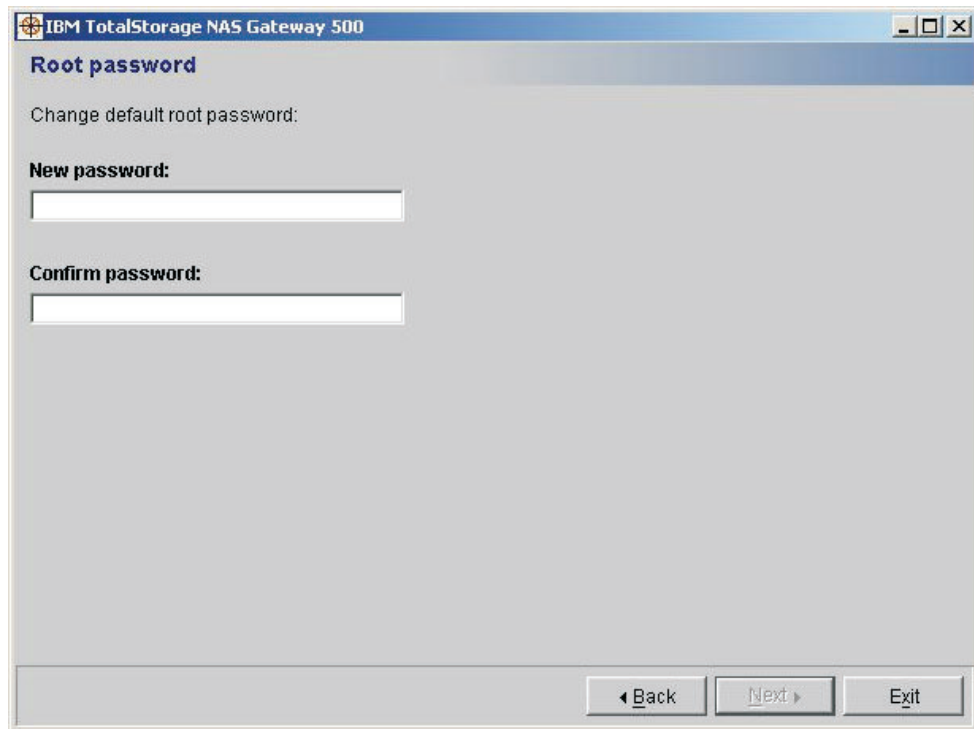
The screenshot shows a window titled "IBM NAS Gateway 500" with a "Date and time" panel. The panel contains the following fields and controls:

- Date:** A dropdown menu for the month (currently "November"), a spin button for the day (currently "4"), and a spin button for the year (currently "2003").
- Time:** Spin buttons for the hour (currently "11"), minute (currently "01"), and second (currently "15"). Radio buttons for "AM" (selected) and "PM".
- Time zone:** A dropdown menu (currently "Mountain U.S. (CUT-7)").
- Note:** "Changes to time zone will not take effect until the next system reboot."
- DST:** A checkbox labeled "Time zone observes daylight saving time (DST)".
- Master time synchronization server (IP address):** An empty text input field.
- Buttons:** "Help", "Next >", and "Exit".

Figure 9. Set Date and Time panel

If you enabled Remote Mirroring at setup, an additional panel follows the Set Date and Time panel. This panel allows you to set the date and time for the remote site.

2. Use the root password panel to enter the new password that you have chosen for the root password. Reenter the same password to confirm. Click **Next**.



IBM TotalStorage NAS Gateway 500

### Root password

Change default root password:

**New password:**

**Confirm password:**

◀ Back   Next ▶   Exit

Figure 10. Set root password panel



3. Use the NAS Administrators Wizard panel to add or delete NAS administrators. NAS administrators are privileged users on the NAS Gateway 500 who can perform administrative tasks, such as configuring clustering, or Windows file serving. They are not given root access to the NAS Gateway 500. They operate within a protected shell with specialized functions that provide simplified interfaces for NAS Gateway 500 management. Because they are limited to a protected shell, they only have access to commands that allow for the day-to-day management of the NAS Gateway 500.

**Note:** This is the preferred method for managing the NAS Gateway 500.

- a. If you click the **Add** button, the Add NAS administrator panel appears.
  - 1) Enter a user ID and optionally the full name of the NAS administrator. The user ID can be up to 8 alphanumeric characters or underscores.
  - 2) Enter the password you want the NAS administrator to use. Confirm the password.
  - 3) Click **OK** and you are returned to the window where you see the newly created NAS administrator in the text box.
- b. To remove an administrator from the list, click an existing administrator and click **Delete**.
  - 1) The Delete administrator dialog box is displayed asking you if you are sure you want to delete the specified administrator
  - 2) Click **OK** if you are sure; the administrator is deleted.
- c. Click **Next**.

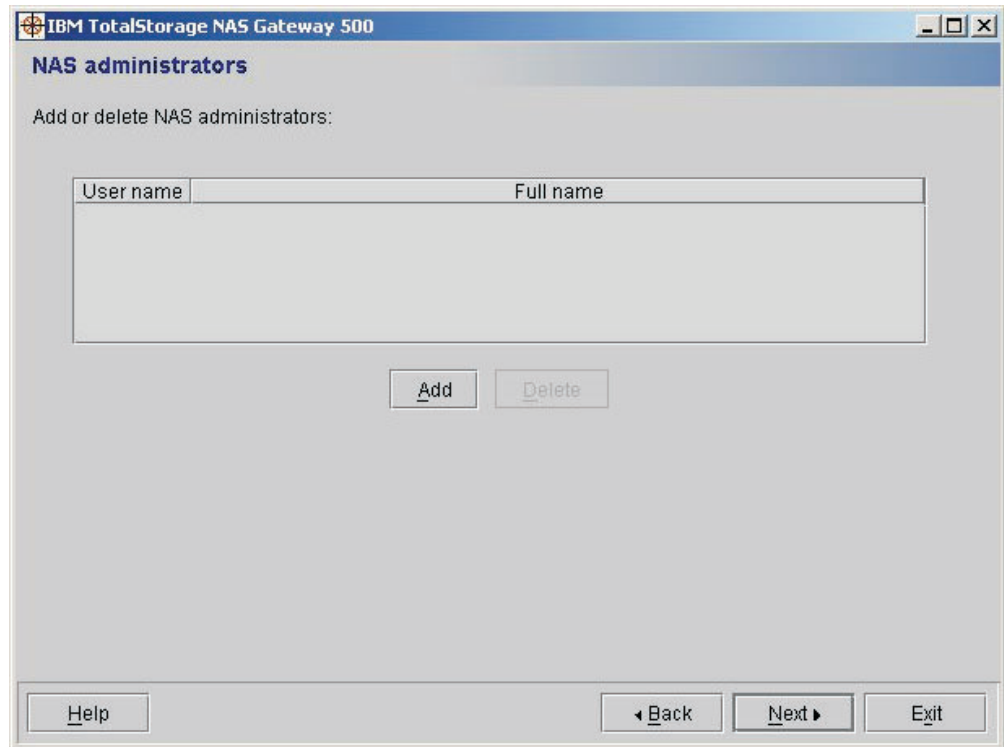


Figure 11. Add or Delete NAS administrators panel

4. If you want to configure your NAS Gateway 500 to authenticate users through the NIS directory service, select **NIS client**. If you do not have a directory service configured or plan to use NIS+ or LDAP, select **None**. Click **Next**.

**Note:** NIS+ and LDAP are configured after initial configuration. See “Directory Services” on page 104.

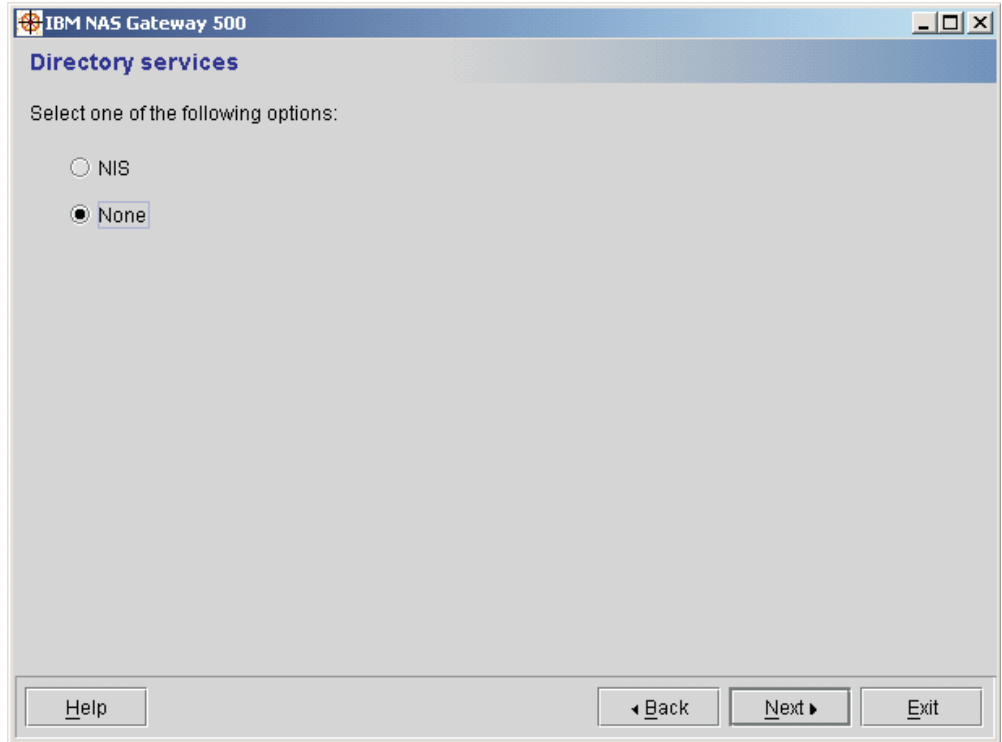


Figure 12. List of Directory Services panel

If you selected NIS client, you need to enter the NIS domain name and the IP address of the NIS server in the following panel and then click **Next**.

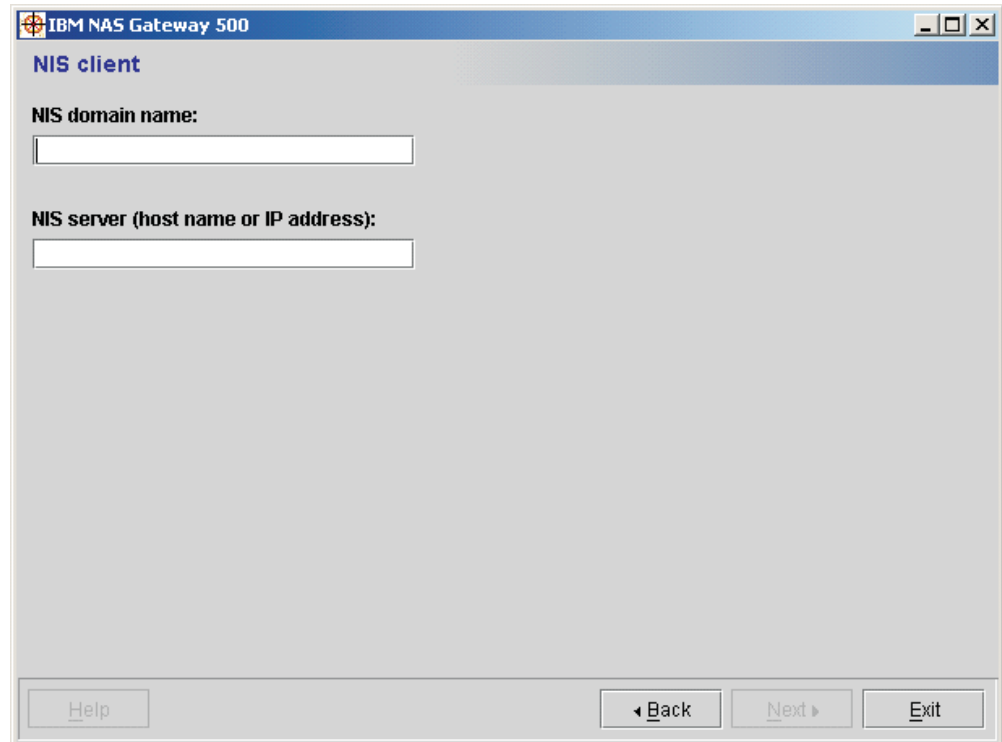


Figure 13. NIS Client configuration panel

5. Use the File access users panel to add or delete users that require file access on the NAS Gateway 500. These are local accounts on the NAS Gateway 500, that have no login privileges and exist only for authentication purposes for ownership of files and directories. It is not necessary to enter all of your file access users at this time.
  - a. If you click **Add**, the Add file access user panel appears allowing input for the file access user ID you want to create.
    - 1) Enter a user ID and optionally the full name of the file access user. The user ID can be up to 8 alphanumeric characters or underscores.

**Note:** The file access user ID cannot be *user*.
    - 2) Enter the password you want the file access user to use.
    - 3) Click **OK** and you are returned to the File access users window where you see the newly created file access user in the text box.
  - b. To remove a file access user from the list, click an existing file access user ID and click **Delete**.
    - 1) The Delete User dialog box is displayed asking you if you are sure you want to delete the specified user ID.
    - 2) Click **OK** if you are sure and the file access user is deleted.

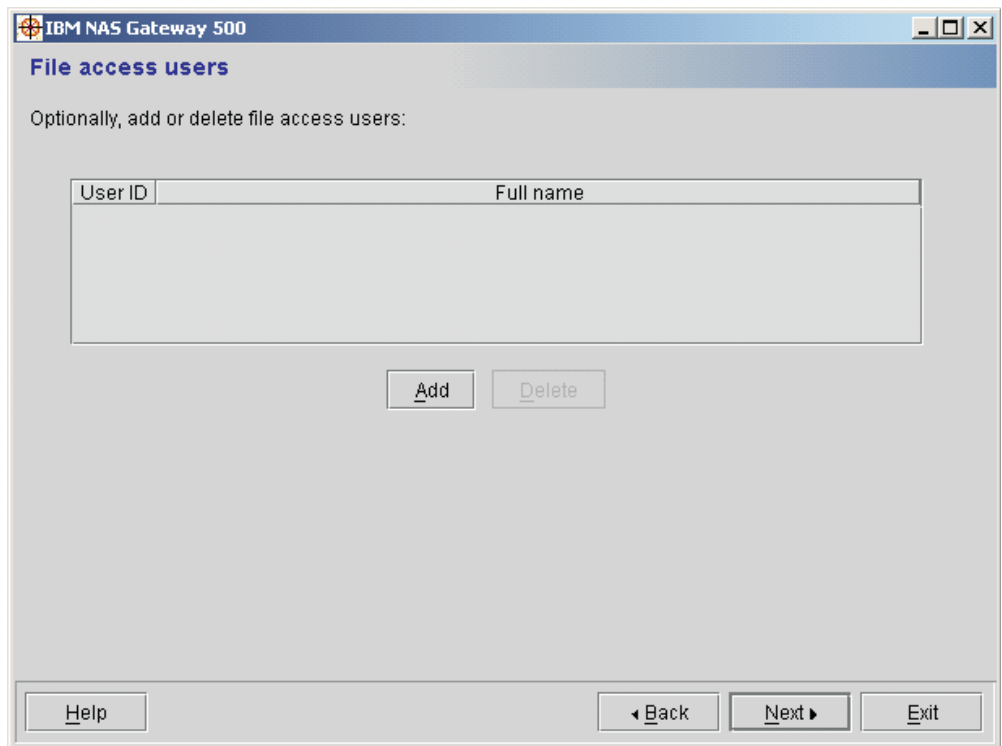


Figure 14. File access users panel

6. After adding file access users and clicking **Next**, you have completed the general setup portion of the initial configuration, and you are automatically entered into the next portion of initial configuration. If you selected clustering in the Feature Selection Wizard, you begin the Cluster Configuration Wizard (see Chapter 10, “Using the Cluster Wizard,” on page 43). If you did not select clustering, you begin the Network Configuration Wizard (see Chapter 9, “Using the Network Configuration Wizard,” on page 41).



## Chapter 9. Using the Network Configuration Wizard

If you did not select clustering in the Feature Selection Wizard, the Network Configuration Wizard allows the network configuration of your single-node NAS Gateway 500. This wizard is for single-node gateways only. See Chapter 10, “Using the Cluster Wizard,” on page 43 for information on network configuration using clustering and Remote Mirroring nodes.

Use the following panel to configure the network on your single-node NAS Gateway 500:

Host name: SW03

DNS domain name: tigerteam.com

Primary DNS server (IP address): 192.168.3.100

Secondary DNS server (IP address):

Default gateway: 192.168.3.100

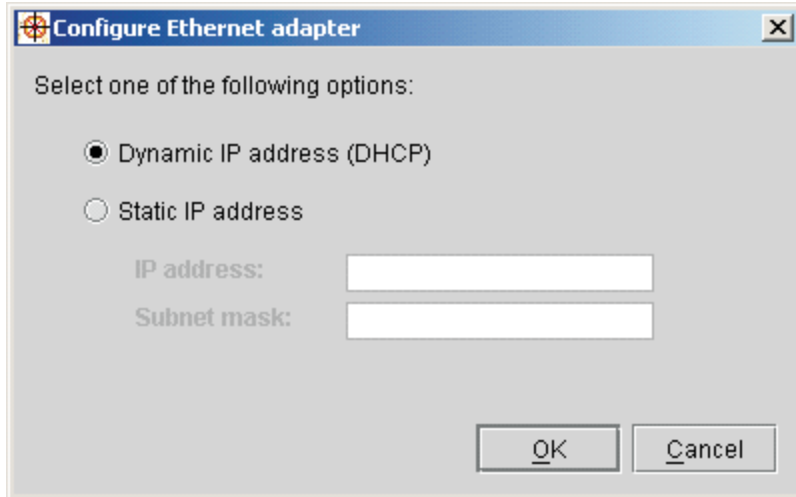
Configure Ethernet interfaces:

Card/Port	IP address	Subnet mask
Gigabit Ethernet-SX PCI-X Adapter (Card Slot 2 Port 1)		
2-Port Gigabit Ethernet-SX PCI-X Adapter (Card Slot 4 Port 1)		
2-Port Gigabit Ethernet-SX PCI-X Adapter (Card Slot 4 Port 2)		
2-Port 10/100/1000 Base-TX PCI-X Adapter (Card Slot 6 Port 1)		
2-Port 10/100/1000 Base-TX PCI-X Adapter (Card Slot 6 Port 2)		

Figure 15. Network configuration panel

1. Enter the host name. Refer to your worksheets.  
The host name can be from one to 31 alphanumeric or underscore characters only; although you cannot begin the host name with a number. The names must be unique; if the names are longer than 24 characters, at least one of the first 24 characters must be unique.
2. The primary and secondary Domain Name Server (DNS) addresses are used to resolve host names into dotted IP addresses. Enter the DNS address or addresses provided by your network administrator.
3. To launch the Link Aggregation Wizard, click **Configure Link Aggregation**. (See Chapter 14, “Using the Link Aggregation Wizard,” on page 67 for information on the Link Aggregation Wizard.)
4. Select the adapter you want to configure and click **Edit**.

5. Use the Configure Ethernet adapter panel to select a static or dynamic address. If you select static, you can then enter the IP address and subnet mask for the specified adapter. Click **OK** to complete the change and return to the Network configuration panel.



*Figure 16. Static or dynamic IP address selection panel*

6. If you selected CIFS in the Feature Selection Wizard, clicking **Next** starts the CIFS Wizard. If you did not select CIFS, the Volume Wizard is displayed.



## Chapter 10. Using the Cluster Wizard

Use the Cluster Wizard to complete the clustering and network configuration when clustering is selected in the Feature Selection Wizard. The *IBM TotalStorage NAS Gateway 500 Planning Guide* contains worksheets to simplify the entering of the required IP addresses.

1. The first panel is the Cluster Setup panel:

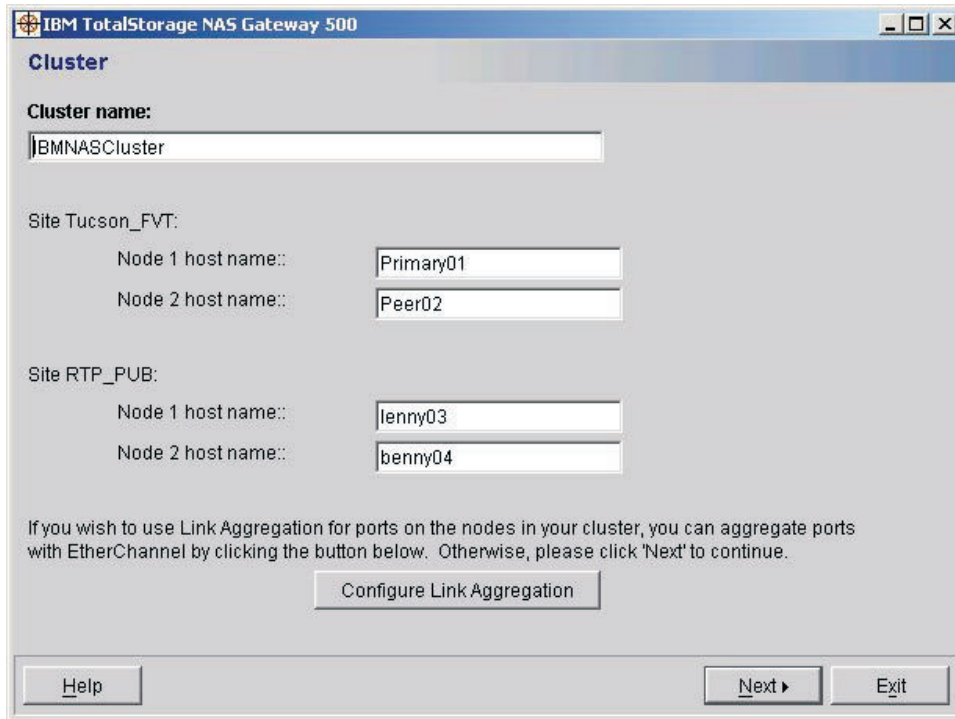


Figure 17. Cluster Setup

This panel prompts you for cluster name and host names. The panel format depends on whether you specified Remote Mirroring (and, if so, the topology of the cluster). Site names appear only for remote mirrored configurations. Click **Configure Link Aggregation** to launch the Link Aggregation Wizard.

A cluster name is required; two to four host names are also required, depending on the number of nodes you selected. The cluster name uniquely identifies the cluster. For Remote Mirroring, this cluster name applies to all nodes at both sites. Without Remote Mirroring, the cluster name applies to both nodes. A well-chosen name is especially useful when multiple clusters are defined on a network.

The cluster name can be from one to 31 alphanumeric characters; underscores are allowed, although you cannot begin the cluster name with a number. The host names must be unique; if the names are longer than 24 characters, at least one of the first 24 characters must be unique.

Click **Next**.

2. The next panel, Cluster for node with Remote Mirroring, appears once for each node in the cluster, in the following order:
  - a. Local primary node (the node you are currently logged into)

- b. Local peer node (if present; a peer node is always present when using local clustering without Remote Mirroring)
- c. Remote primary node (if Remote Mirroring is used)
- d. Remote peer node (if present)

Each panel configures the networking cluster parameters. If you selected Remote Mirroring, Figure 18 appears. If you did not select Remote Mirroring, Figure 19 on page 45 appears. The following fields appear only if the Remote Mirroring feature is selected:

- Mirrored Volumes File serving IP addresses
- Mirroring Mode
- Remote Priority Node

**Cluster for node Primary01**

Subnet mask: 255.255.255.0

File serving IP addresses: (non-mirrored volumes) 192.168.3.83

Enable fallback (automatically restore file serving)

**Mirrored Volumes**

File serving IP addresses: 192.168.3.84

Mirroring Mode: Synchronous Remote Priority Node: Jenny03

Boot Adapter: 2-Port Gigabit Ethernet-SX PCI-X Adapter (Card Slot 4 Port 2)

Boot IP address: [Empty]

[Add] [Delete]

Boot Adapter	Boot IP address
Gigabit Ethernet-SX PCI-X Adapter (Card Slot 2 Port 1)	10.11.0.1
2-Port Gigabit Ethernet-SX PCI-X Adapter (Card Slot 4 Port 1)	10.12.0.1

[Help] [Back] [Next] [Exit]

Figure 18. Cluster for node with Remote Mirroring

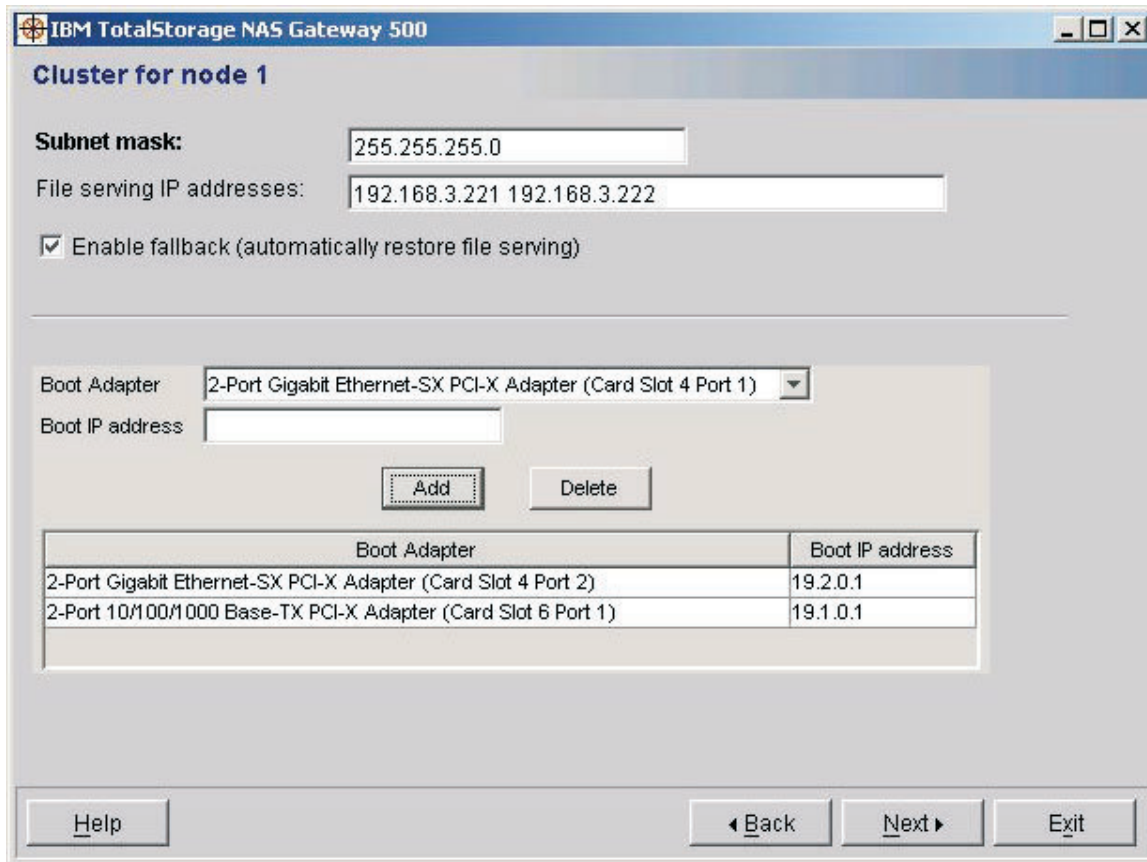


Figure 19. Cluster for node without Remote Mirroring

On these panels:

- a. Enter the subnet mask for the cluster. The subnet mask is combined with an IP address to define the subnet. The subnet mask is the same for every IP address in the cluster and should be the subnet mask assigned to your client network.
- b. Enter the file serving IP addresses. File serving IP addresses are used by clients to gain access to the NAS volumes. These IP addresses can be on the same or different subnets, but all file serving IP addresses must be on subnets exclusive to all boot IP addresses. When specifying multiple file serving IP addresses in the same box, use a space to separate each IP address.

For Remote Mirroring, there are two sets of file serving IP addresses: one for non-mirrored volumes and one for mirrored volumes. Without Remote Mirroring, only one set is specified. If no file serving IP addresses are specified, then this node is in standby mode and no files are served. If a different node fails, then the file serving duties from the failed node can be transferred to this node, changing it from standby to active mode. In every cluster, one active node must be defined.

- c. Click **Enable fallback (automatically restore file serving)** if you want to enable the node to automatically reintegrate resources that had previously failed over to its local peer node. If using Remote Mirroring, this checkbox does not apply to the case of site failover and fallback.

- d. For remotely mirrored volumes, enter the file serving IP addresses for serving the mirrored volumes. These IP addresses must be different from the file serving addresses for non-mirrored volumes.
- e. For remotely mirrored volumes, choose one of the following mirroring modes:
  - Synchronous mirroring: Data is written first at the remote site, and then at the local site. Further processing is blocked until both writes are complete.
  - Mirror write consistency: Data is written to the local disk concurrently with the copy to the remote site. This increases the performance of the mirror. The write request does not return to the application until both the local and the remote writes are complete.
  - Asynchronous mirroring: Data is written at the local site and is queued to be sent to the remote site. Input can continue at the local site while the previously entered data is being mirrored.
- f. If using Remote Mirroring, you must also choose a remote priority node. The priority node is used to determine which node of a remote site takes over in case of a local site failure.

If the local site has two nodes named L1 and L2 and two remote nodes named R1 and R2, where R2 has been designated the priority node for the local node L1, then:

If L1 fails, L2 takes over.  
Then if L2 fails, R2 takes over.  
Then if R2 fails, R1 takes over.

**Note:** In the event of site failure, refer to Appendix C, “Remote Mirroring problem determination,” on page 295.

Each node at a site has a node at the other site assigned as the remote priority node; if the other site has only a single node, then that node is the remote priority node.

- g. Use the drop-down menu to select the adapter port for which you want to assign a boot IP address. These are base IP addresses assigned to the Ethernet ports to be used in the cluster. Refer to the following guidelines when configuring the boot IP addresses:
  - They are not for direct client access.
  - At least two and no more than eight Ethernet ports must be assigned Boot IP addresses on each node.
  - They must not conflict with another IP address on the network.
  - They must be on different subnets on a given node.
  - They cannot be on the same subnet as any file serving IP addresses within the same cluster.

After selecting the port to use, enter the IP address and click **Add**. The new boot IP address and port are added to the list. Add at least two boot IP addresses; add no more than eight.

- h. Click **Next**.

3. If a node has a boot adapter that is on a different subnet from all the boot adapters on another node, the Static Routes Wizard will be launched before the Synchronize Cluster panel appears, so that static routes to the other subnet or subnets can be configured.

**Attention:** If static routes are necessary, it is important to properly configure the routes. Failure to do so could result in problems synchronizing the cluster. See Chapter 11, “Using the Static Routes Wizard,” on page 51.

4. The Synchronize cluster panel appears:

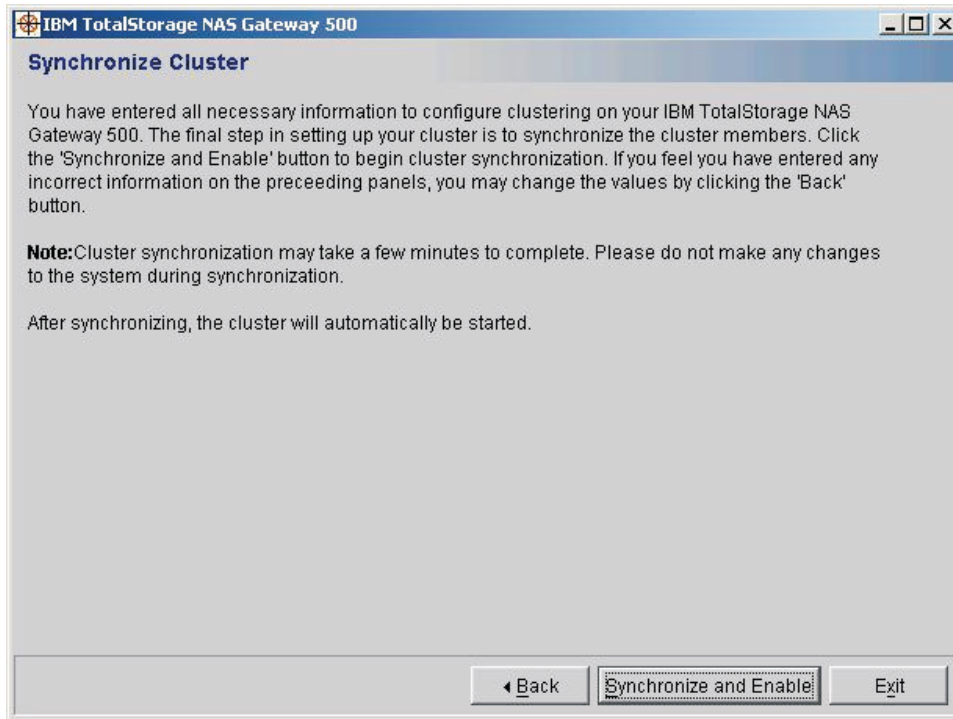


Figure 20. Synchronize cluster

When you have completed cluster configuration for all nodes, you have entered all necessary information to configure clustering on your NAS Gateway 500. The final step in setting up your cluster is to synchronize the cluster nodes. If you feel you have entered any incorrect information on the preceding panels, you can change the values by clicking **Back**.

Click **Synchronize** to begin cluster synchronization. This initial synchronization process takes several minutes to complete. Subsequent synchronizations will be faster. If Remote Mirroring is enabled, the cluster is synchronized and enabled at the end of initial configuration; otherwise, the cluster is enabled (started) after this synchronization is successful.

5. The Node network configuration panel appears next. There is one panel for each node in the cluster. These panels specify the network configuration for all remaining Ethernet ports that were not assigned to the cluster. These ports cannot be used to serve highly available files, because the ports are not a part of the cluster and will not fail over if the node becomes inaccessible. They are better suited for administrative and service uses.

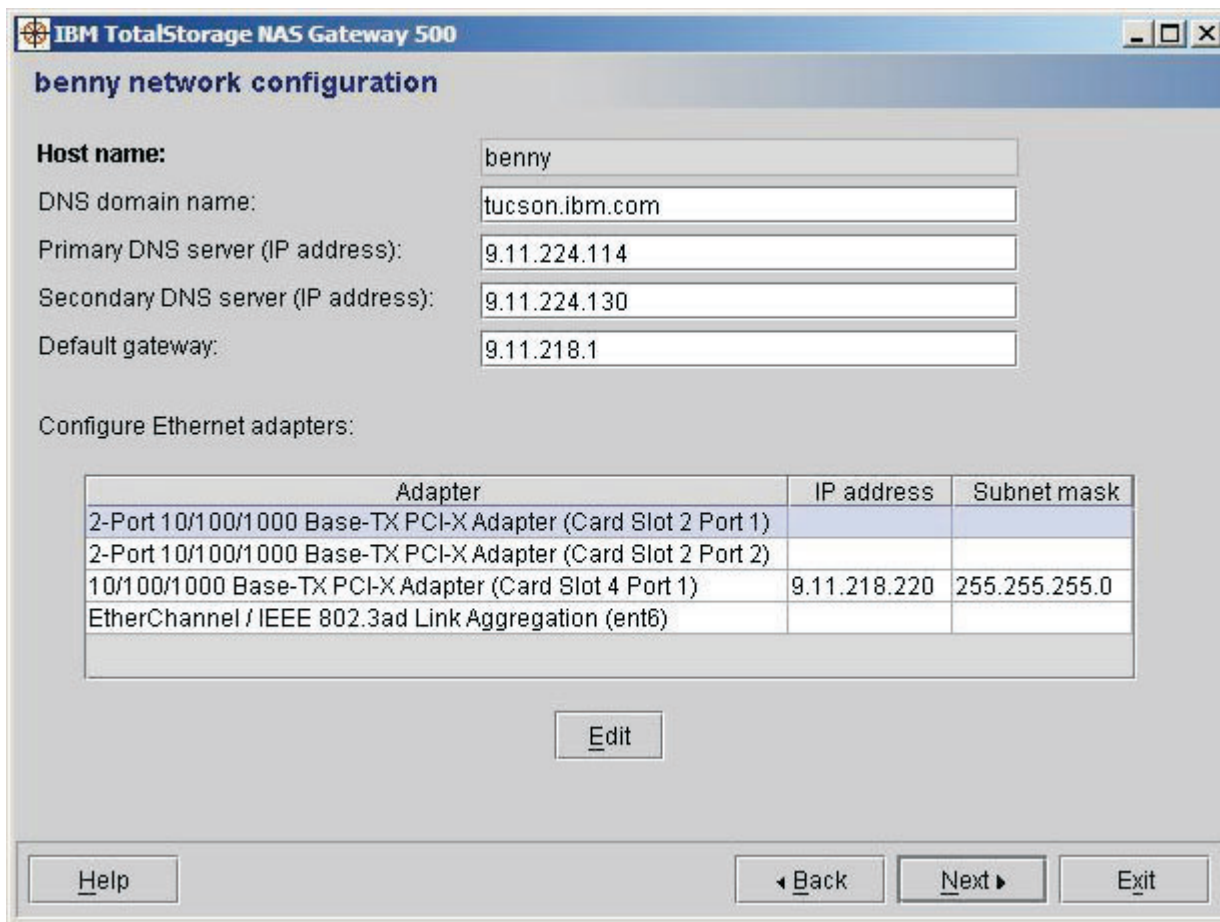


Figure 21. Network configuration 1

If no Ethernet adapters appear, then click **Next** without entering any configuration parameters. On this panel:

- a. The primary and secondary DNS addresses are used to resolve host names into dotted IP addresses. Enter the DNS address.
- b. Enter the default gateway.
- c. Under the configure Ethernet adapters section, you see a list of adapter ports that have not yet been configured. Select the adapter port you want to configure and click **Edit**. You can configure any or all of the adapter ports in the list.

**Note:** The adapter ports are not part of the cluster. They do not provide fail over, and cannot do cluster file serving. After selecting an adapter port and clicking **Edit**, the configure Ethernet adapters panel appears allowing you to select a static or dynamic address for the specified adapter port.

- 1) If you select static, you can enter the IP address and subnet mask for the specified adapter port.
  - 2) Click **OK** to complete the change and return to the network configuration panel.
- d. Click **Next** to display the next Network configuration panel.

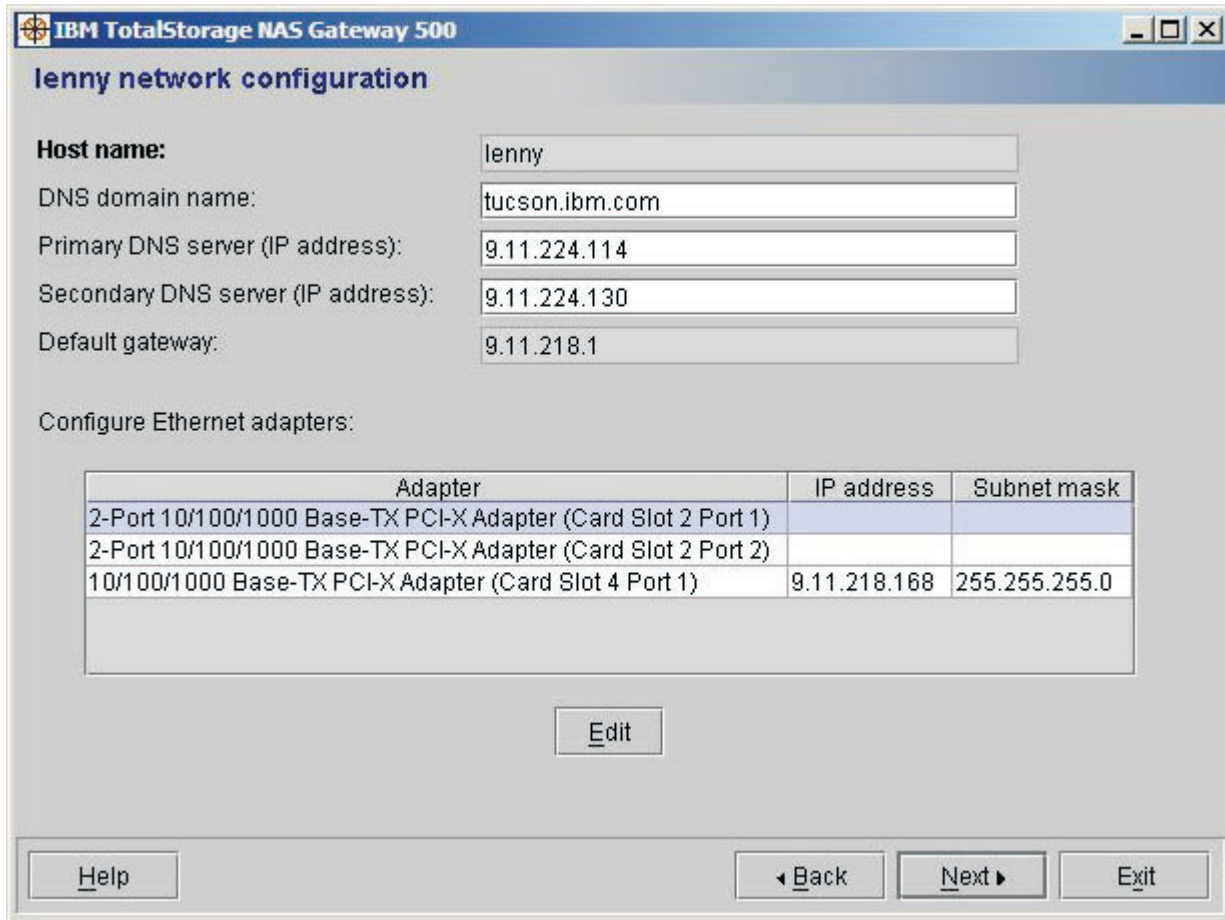


Figure 22. Network configuration 2

- e. Enter the information to configure the node.
6. Click **Next** to configure the network settings for the remaining nodes in the cluster.
7. Click **Next** after you complete all nodes in the cluster. If you are doing initial configuration, the Static Routes Wizard starts automatically.





## Chapter 11. Using the Static Routes Wizard

The Static Routes Wizard allows you to create static routes between different subnets, at either the local or the remote site.

**Note:** Adding a route on only one node at a site is not supported through this wizard; you must do that with the **mkroute** command. Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for information about the **mkroute** command.

If you do not want to configure a static route at this time, click **Skip** to continue initial configuration.

When you run the wizard, you see the following panels:

1. The first panel is the Configure Static Routes panel.  
You are asked for the following information:

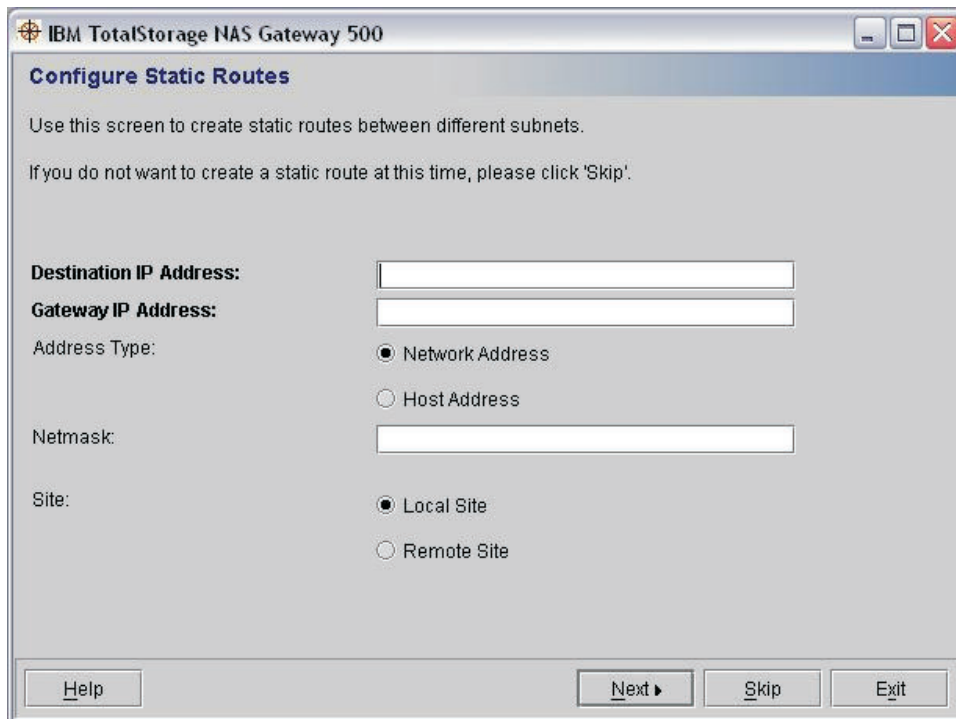


Figure 23. Configure static routes

- Destination IP address
- Gateway IP address: The IP address of the gateway that you use to reach the destination network.
- Address type (network or host): Specifies whether the destination IP address is a host address or a network address.
- Netmask: This field is available only if the destination IP address is a network address rather than a host address. If the address type was *network*, this is the netmask of the network you specified in the destination IP address. If the address type was *host*, this is blank.
- Site (local or remote): This field is available only if remote mirroring is enabled. This specifies whether the route should be added on the node or

nodes at the local site, or on the node or nodes at the remote site. The route will be added on all nodes at the specified site.

Fill in the required fields and click **Next**.

2. A panel appears saying that you have successfully configured a static route. If you want to configure another static route, click **Configure Another Static Route**. Otherwise, click **Next** to continue initial configuration.

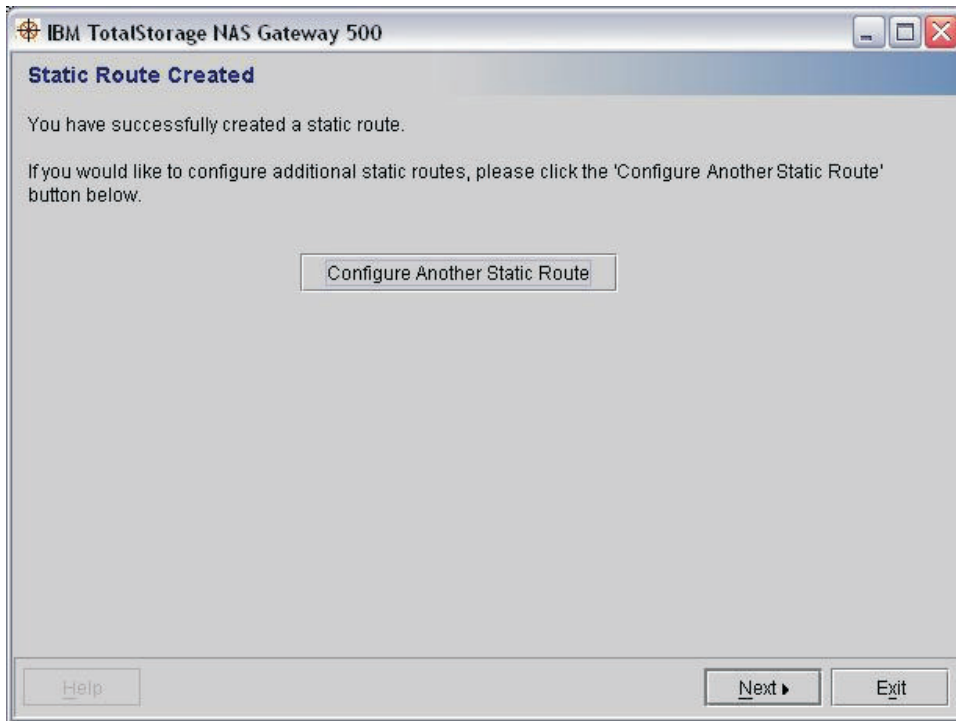


Figure 24. Static route created

---

## Chapter 12. Using the CIFS Wizard

**Note:** The CIFS wizard is started only if CIFS was selected in the Feature Selection Wizard.

The CIFS Wizard configures the NAS Gateway 500 to provide file sharing services to your Microsoft Windows-based clients. This wizard:

- Configures the CIFS server name and workgroup
- Specifies WINS (optional)
- Configures CIFS share users

The CIFS panels differ depending on the system configuration.

If Remote Mirroring is enabled, you are presented with a panel entitled Local CIFS server that lists the nodes for the local site. After entering the settings and clicking **Next**, you are presented with a panel, Remote CIFS server, that lists the nodes for the remote site. This panel is different from the panel displayed during a regular cluster configuration.

If clustering without Remote Mirroring, then there is only one CIFS panel with settings for two servers. A single-node gateway system has a single CIFS panel with fields for one node. Supply the information for these fields using the following descriptions:

1. Use the CIFS server panel to enter the name of your server, a server description, and the domain group.
  - a. The server name is the name by which your Windows clients access your file shares. It is set to the host name of your computer by default but can be changed. A server name can be no longer than 15 characters.
  - b. The server description appears next to your server name in network places and generally contains a short description of the share location, department or type.
  - c. The domain or workgroup name specifies the location of the CIFS share in network places. The name should be applicable to the environment the shares are used in, for example, a department name or office number.
  - d. Click **Next** to continue configuring CIFS.

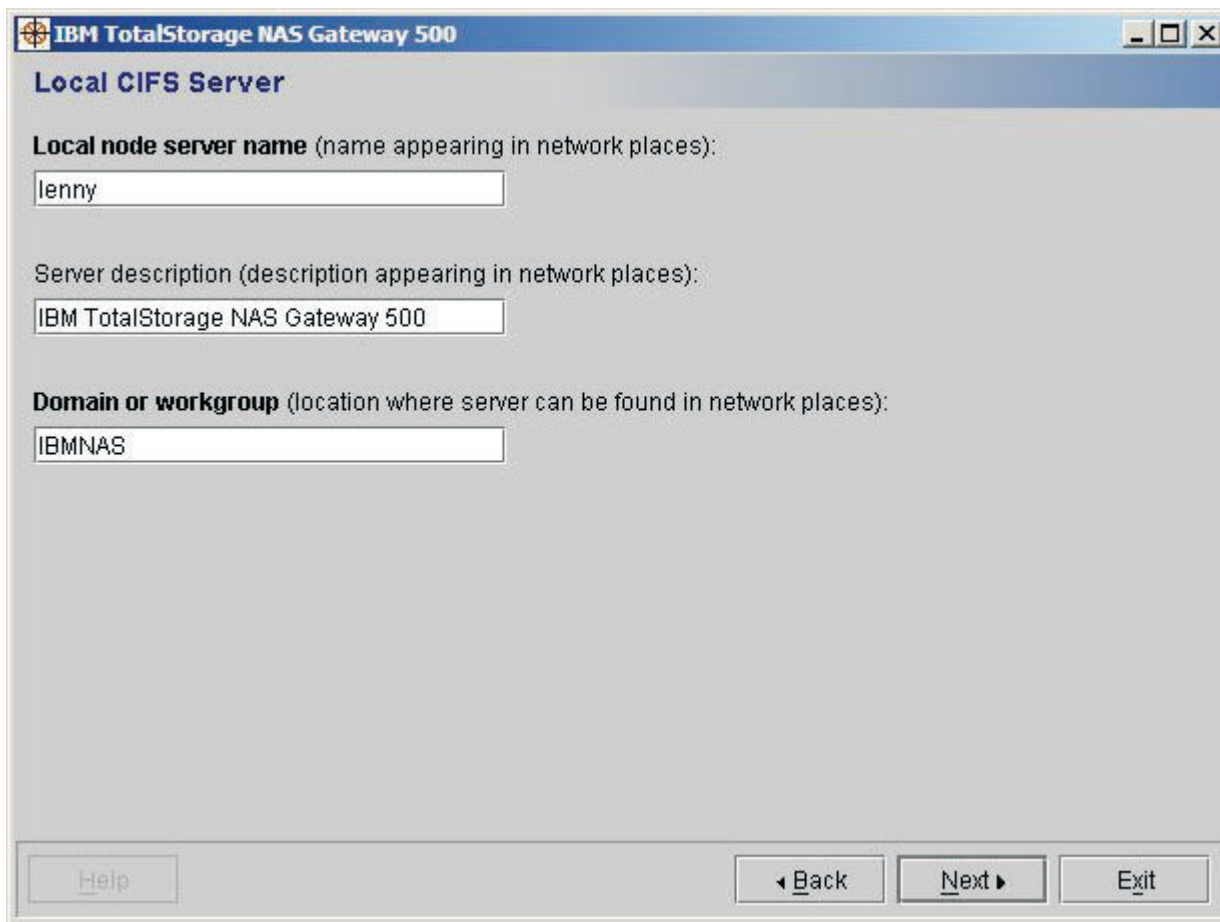


Figure 25. Local CIFS Server

2. If you are using Remote Mirroring, after you see the local CIFS server panel, a Remote CIFS server panel appears. The same fields are required; fill them in accordingly with the remote server information.
3. The Windows Internet Name Service (WINS) is an advanced NetBIOS name server. It is used to map IP addresses to more human-readable hostnames. The CIFS Setup Wizard allows you to specify WINS servers by entering one or two IP addresses of the servers into the fields shown. If you do not want to use WINS, leave the fields blank and click **Next**. If you want to use WINS, enter the server IP address or addresses and click **Next**.

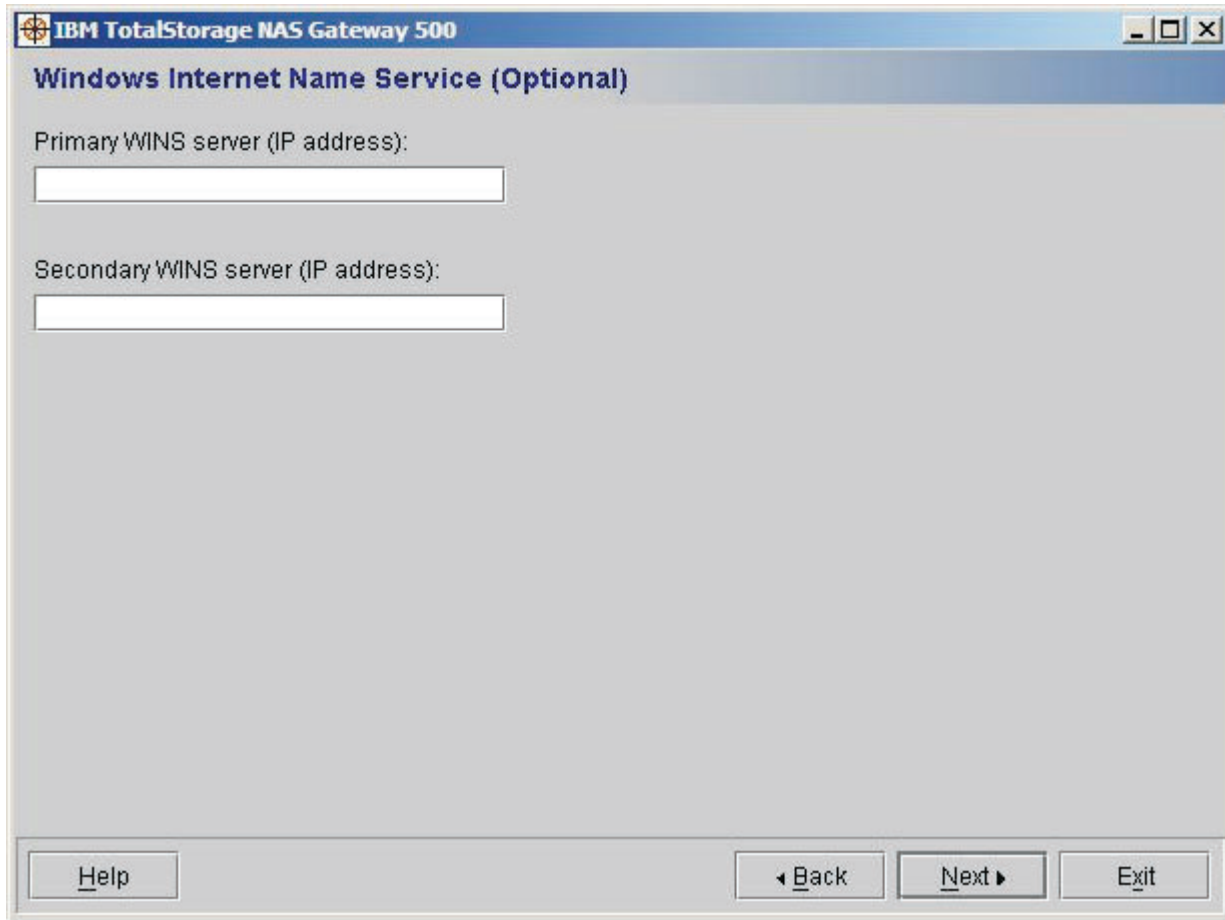


Figure 26. Windows Internet Name Service

4. The CIFS authentication panel is used to specify how you want the NAS Gateway 500 to authenticate Windows users that have access to defined shares. Windows users can be authenticated in two ways:
  - Active Directory or NT4 Domain - When a user enters their username and password into a Windows computer, they are passed through to a central server, which authenticates the user.
  - Locally on each machine - Each client keeps track of the users that log into it. When a user types their username and password, it is verified on the client on which it was entered. Password encryption can be handled three ways:
    - a. No Encryption - Only plain text passwords are accepted.
    - b. Only Encryption - Only encrypted passwords are accepted.
    - c. Negotiate Encryption - Clients can negotiate either plain text or encrypted passwords.

Use the pull-down box to specify the desired encryption.

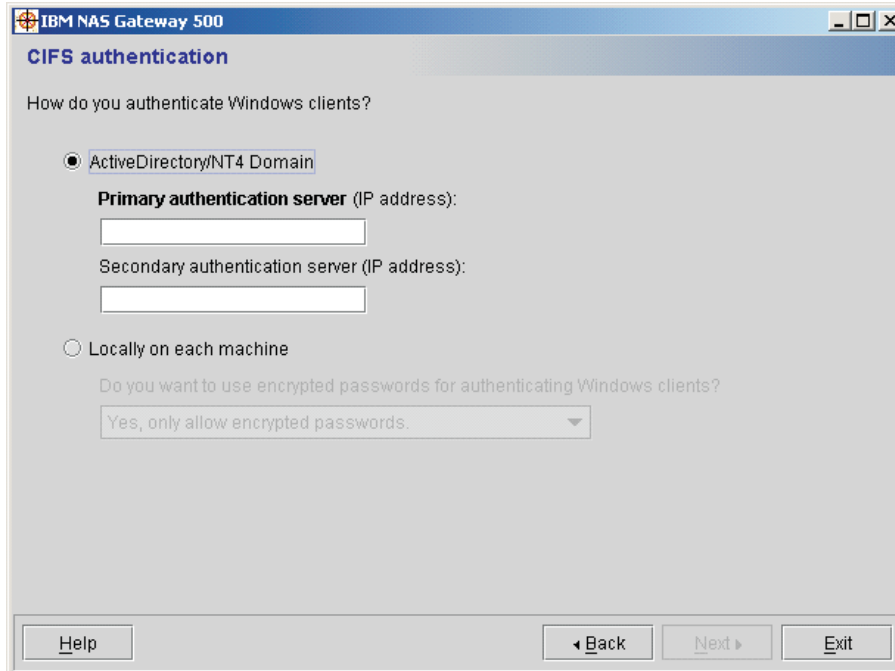


Figure 27. CIFS User Authentication panel

5. If you selected Active Directory on the previous panel, then the CIFS Local users panel appears. Use the CIFS Local users panel to select how you want to create local user accounts. Click your selection and click **Next**.

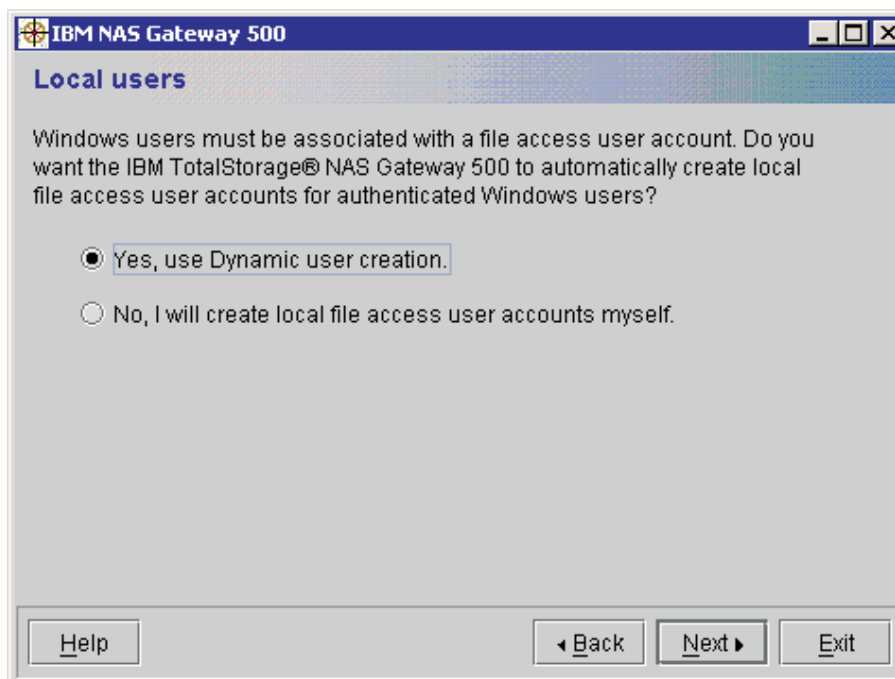


Figure 28. CIFS Local users panel

6. The Confirm CIFS settings panel allows you to confirm your CIFS settings before continuing. If your settings are correct, click **Next**.

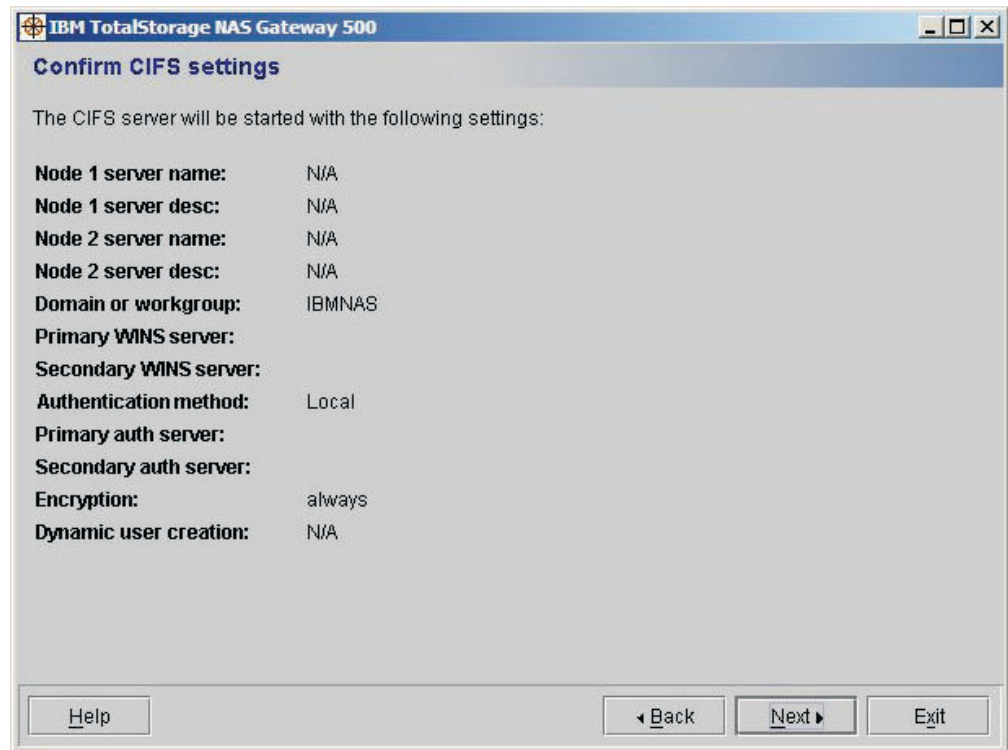


Figure 29. Confirm CIFS settings panel





---

## Chapter 13. Using the Volume Wizard

This chapter describes how to create NAS volumes on your NAS Gateway 500. NAS volumes are disk space on external disk storage system that serve files to client machines.

**Attention:** External storage must be preconfigured on the devices before you can create NAS volumes on the NAS Gateway 500. This is done through standalone clients using the software provided by the storage manufacturer.

The NAS Gateway 500 supports Subsystem Device Driver (SDD); unlike the other drivers, it is not preinstalled. If you have external storage attached that requires the SDD, exit the Volume Wizard and install the driver (if you have not already done so). Any NAS volume configuration performed prior to the installation of the SDD is lost if the SDD is installed afterward. After the installation of the SDD, you can execute this wizard again to define your NAS volumes (see “Volume Wizard” on page 73 for instructions on running the Volume Wizard again). Refer to *IBM TotalStorage Advanced Configuration and Problem Determination Guide* for information about migrating to the SDD on the NAS Gateway 500.

If your external storage requires entry of the World Wide Name (WWN) for the fibre channel host bus adapters installed in your NAS Gateway 500, it can be obtained by opening a Web browser and entering:

`http://hostname/NAS500GetWWN.html`

Where *hostname* is the hostname you previously entered. If you are setting up a clustered box, see Chapter 10, “Using the Cluster Wizard,” on page 43 for the hostname. If you are setting up a single node gateway, see Chapter 9, “Using the Network Configuration Wizard,” on page 41 for the hostname.

1. The first Volume configuration panel selects the node that owns the NAS volume that you are creating. (To skip this wizard and create NAS volumes later, click **Next** and then click **Skip** on the next panel.)

The node that you select on this panel determines the physical disks that appear on the next panel. This panel reappears for each NAS volume you create.

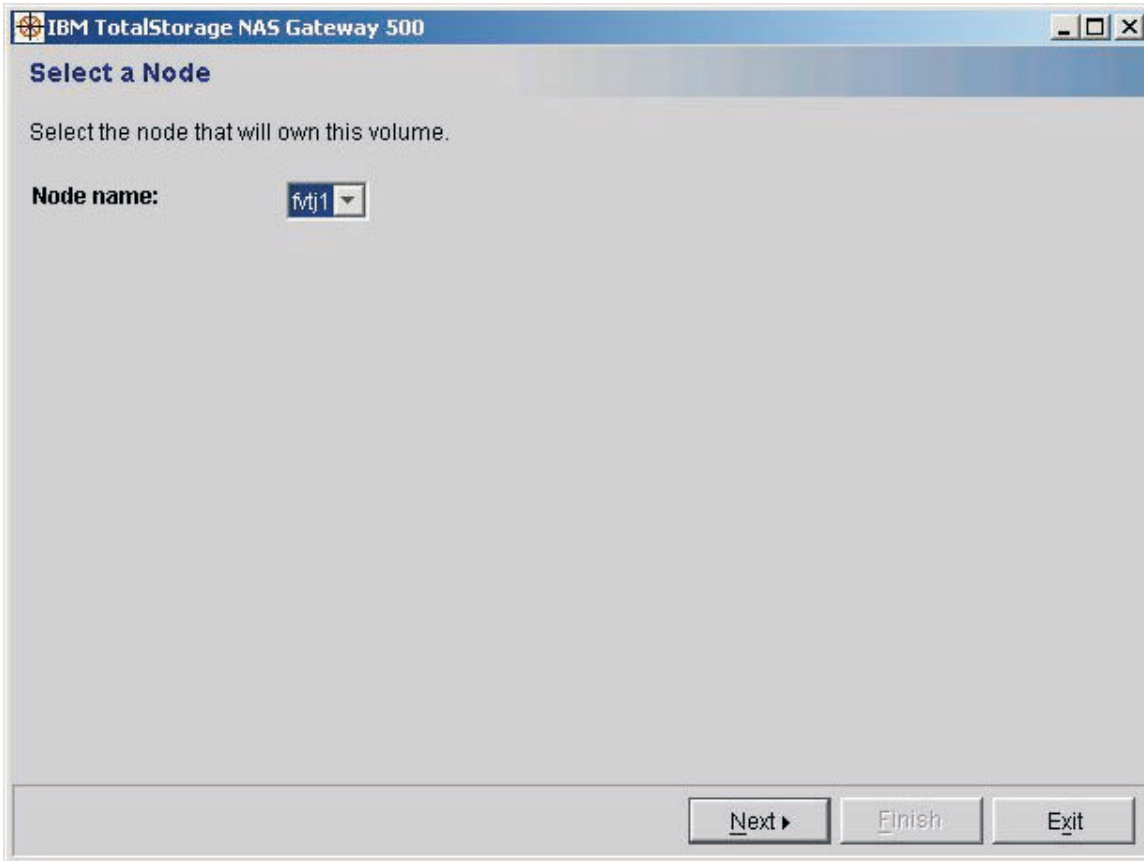


Figure 30. Select a node panel

2. A Volume selection panel appears. A physical volume is the physical hard disk or hard disks that the newly created NAS volume allocates. In the Volume selection panel below, you must select one or more physical volumes from which you want to allocate disk space and click **Add**. Your selection appears in the Selections box. Once you have selected all the hard disks you require for this NAS volume, click **Next**.

**Note:** If you have not configured your external disk storage system, a panel is displayed alerting you to configure your storage prior to running the Volume Wizard. If you would like to configure NAS volumes at a later time, you can click **Skip**.

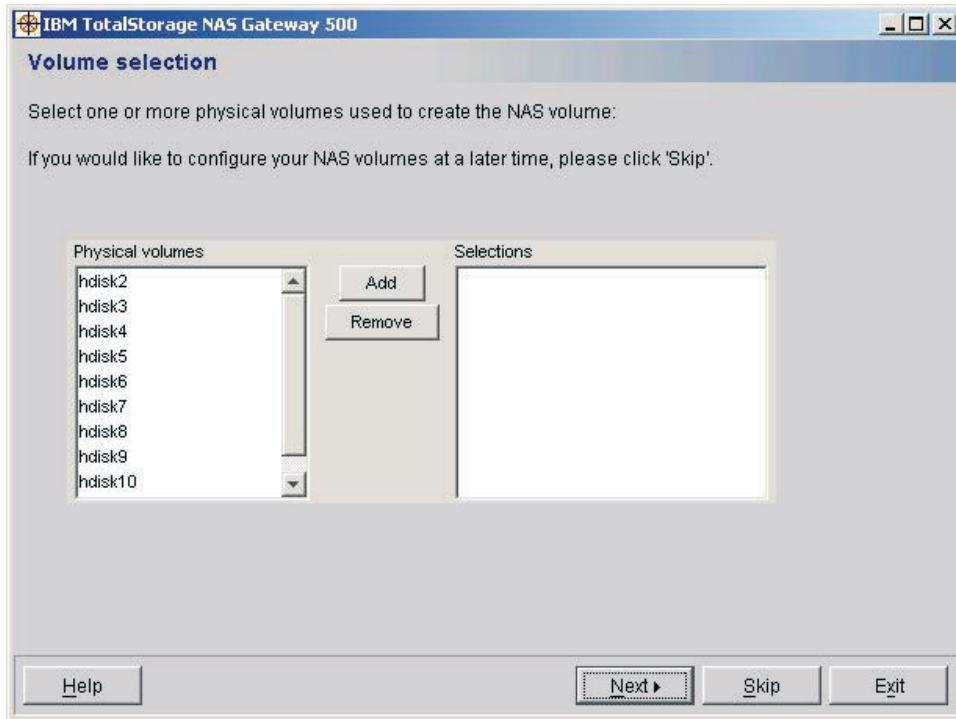


Figure 31. Volume selection panel

3. A Volume configuration panel appears.

The screenshot shows a window titled "IBM TotalStorage NAS Gateway 500" with a "Volume configuration" header. The configuration fields are as follows:

- Volume name:** A text box containing "vol1".
- Hostname:** A drop-down menu showing "benny".
- Cluster name:** A text box containing "NASCluster".
- Maximum number of snapshots:** A scroll box set to "2".
- Snapshot size (percentage of the volume to be reserved for snapshots):** A scroll box set to "10" followed by a "%" symbol.
- Export the volume as a NFS share:** An unchecked checkbox.
- Use snapshot dynamic link default setting:** An unchecked checkbox.
- Create remotely mirrored volume:** A checked checkbox.
- Remote Node:** A drop-down menu showing "lenny".

At the bottom of the window are four buttons: "Help", "Back", "Next", and "Exit".

Figure 32. Volume configuration panel

Use this panel to enter the specifics associated with the NAS volume you are defining.

- a. The Volume name field is for the name you want to use to identify created NAS volumes.

**Note:** When the volume name specified by *volume* is mounted, it will be mounted as */Vols/volume*.

- b. The Hostname drop-down box is the name of the host that owns the volume in a clustered configuration.
- c. The Maximum number of snapshots scroll box is for the maximum number of snapshots that can be allocated on a volume. The maximum number that can be used is 15.
- d. The Snapshot size scroll box is for the percentage of the file system space reserved for snapshots.
- e. The Enable CIFS sharing check box allows you to specify that you want the new NAS volume to be created as a CIFS share. CIFS file serving is an optional feature of the NAS Gateway 500. This feature must be enabled before using CIFS shares.

- f. The Export the volume as an NFS share check box allows you to specify that you want the new volume to be exported as an Network File System (NFS) share.

**Note:** Both CIFS and NFS can be enabled on the same NAS volume.

- g. The Use snapshot dynamic link default setting check box allows you to use the snapshot dynamic link default setting.
- h. The Create remotely mirrored volume check box allows you to create a remotely mirrored volume. This option is only available if remote mirroring was selected during the Feature Selection Wizard.

**Note:** If you do **not** select this check box, the NAS volume creation confirmation panel appears. If you **do** select this check box, the Remote Volume configuration panel appears. If you select to create a remotely mirrored volume, you will need to select a remote node that will be used to list the disks at the remote site.

- i. Click **Next**.
4. A Remote volume configuration panel appears. Use this panel to enter the specifics associated with the volume you are defining. Choose which disks should contain the remote mirror volume (similar to the previous panel) and click **Next**.

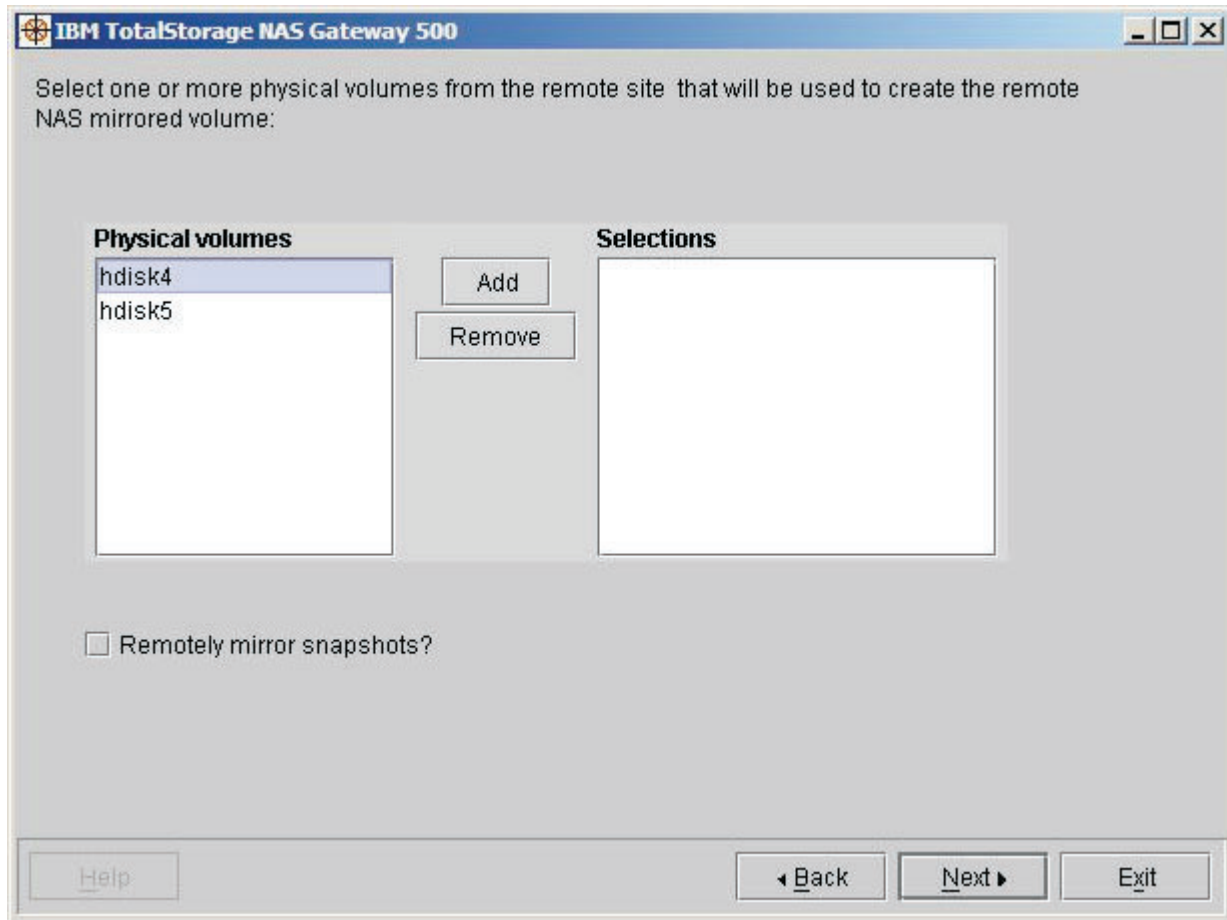


Figure 33. Remote volume configuration panel

5. A NAS volume creation confirmation panel appears. This panel provides information about the NAS volume that you are about to create in the Volume configuration panel. Click **Next**.

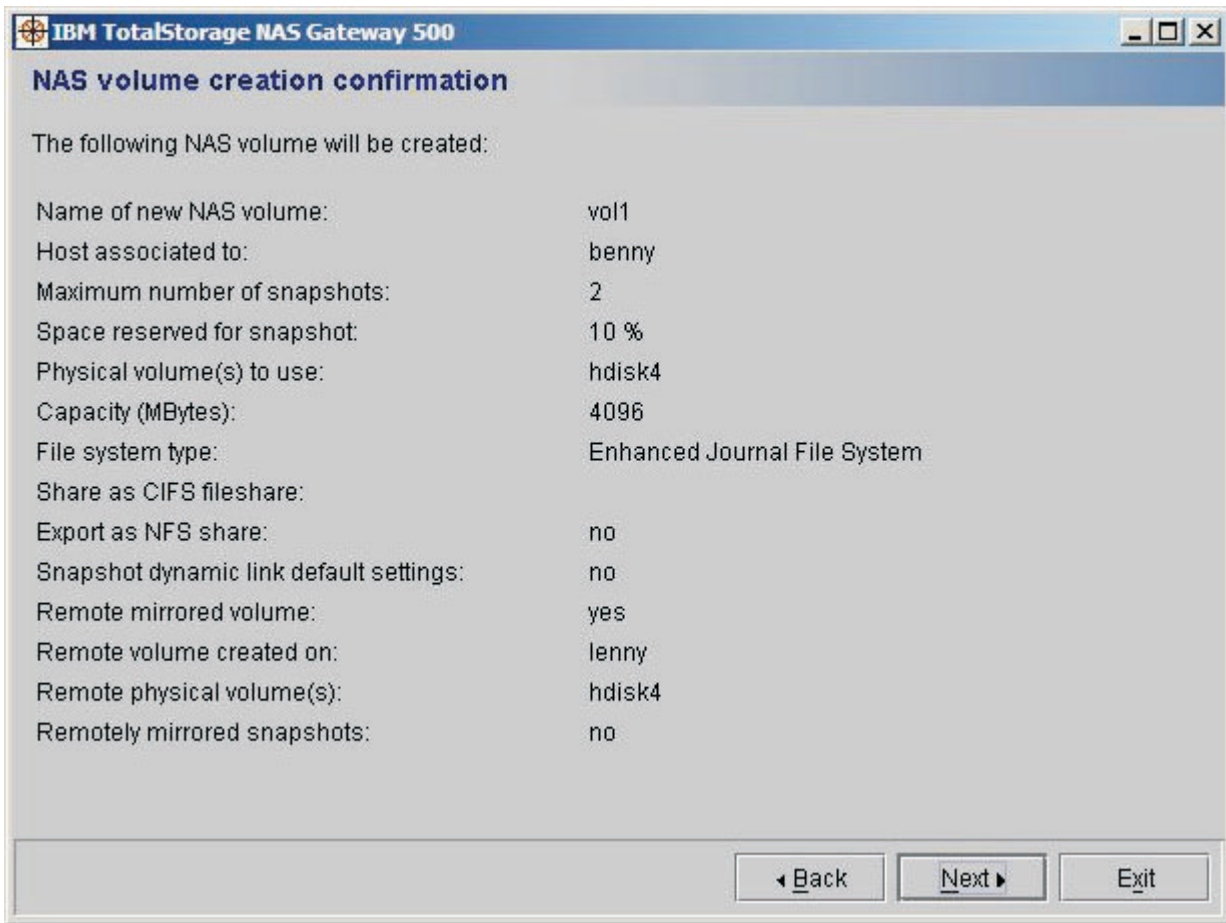


Figure 34. NAS volume creation confirmation panel

6. A NAS volume creation complete panel appears. Use this panel to continue creating additional NAS volumes. To create additional NAS volumes, click **Create another volume**, and you are returned to the Volume configuration panel. If you do not want to create additional NAS volumes, click **Next**.

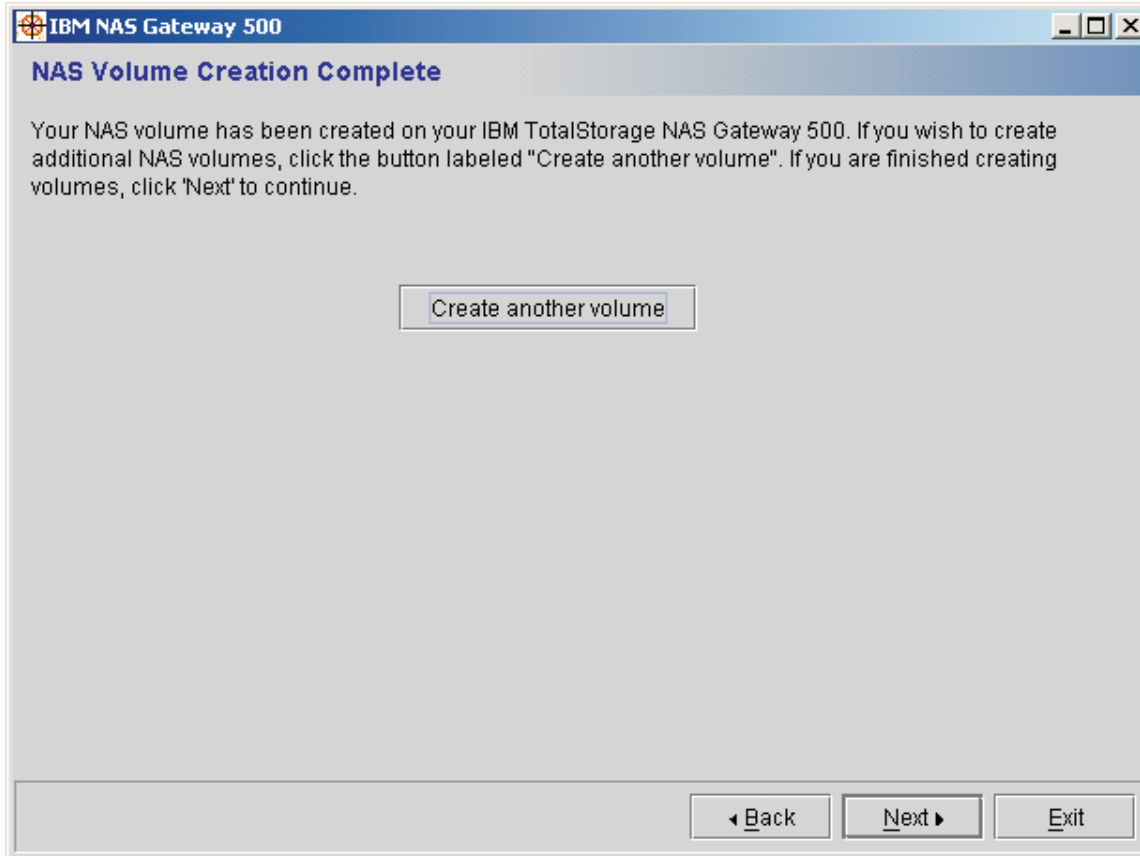


Figure 35. NAS Volume Creation Complete panel

7. Click **Finish** to complete initial configuration and then close the WebSM client.

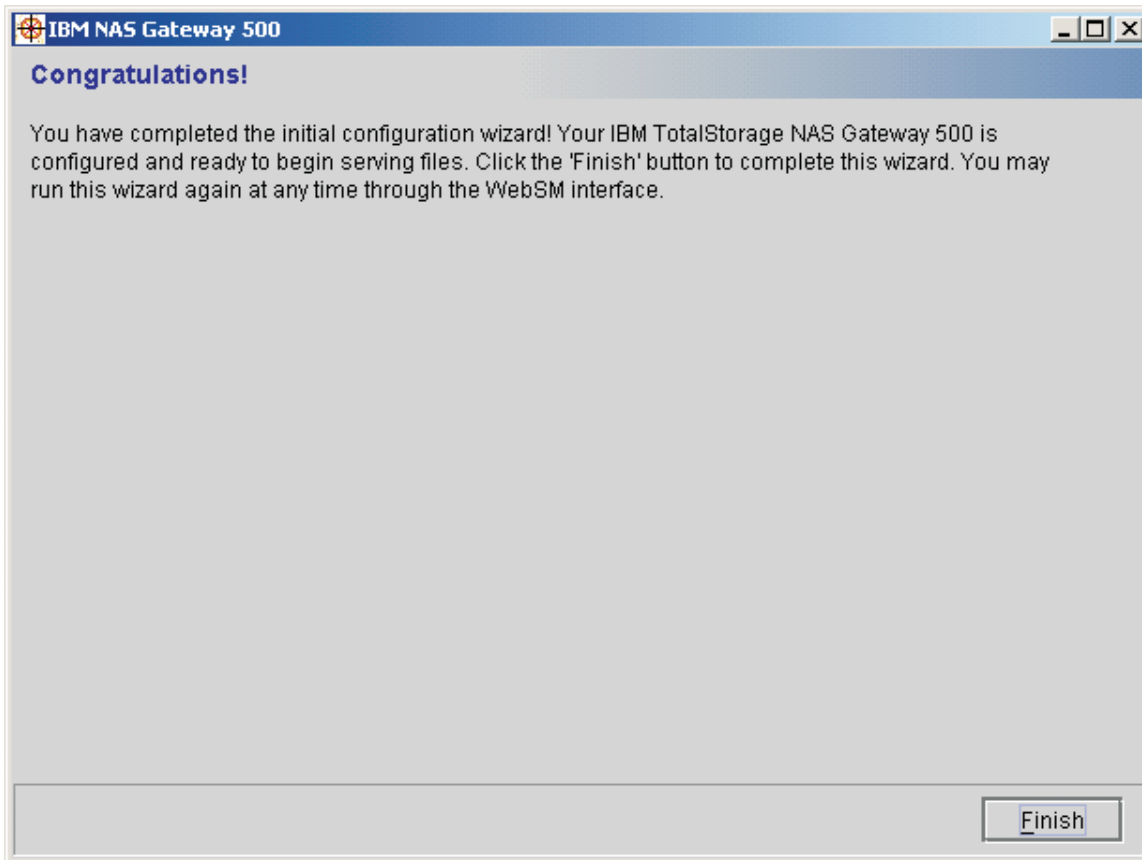


Figure 36. Congratulations panel

**Note:** To rerun any of the individual wizards, use the WebSM NAS System Interface. See Chapter 15, "Running wizards after initial configuration," on page 71 for more information.



## Chapter 14. Using the Link Aggregation Wizard

The Link Aggregation Wizard is optionally called from multiple locations during the initial configuration process. This wizard allows you to select one or more Ethernet interfaces to be used for link aggregation. When you run the wizard, you see the following panels:

1. You are asked to select which Ethernet Adapter ports you want to include in the aggregation. Make your selections and click **Next**.

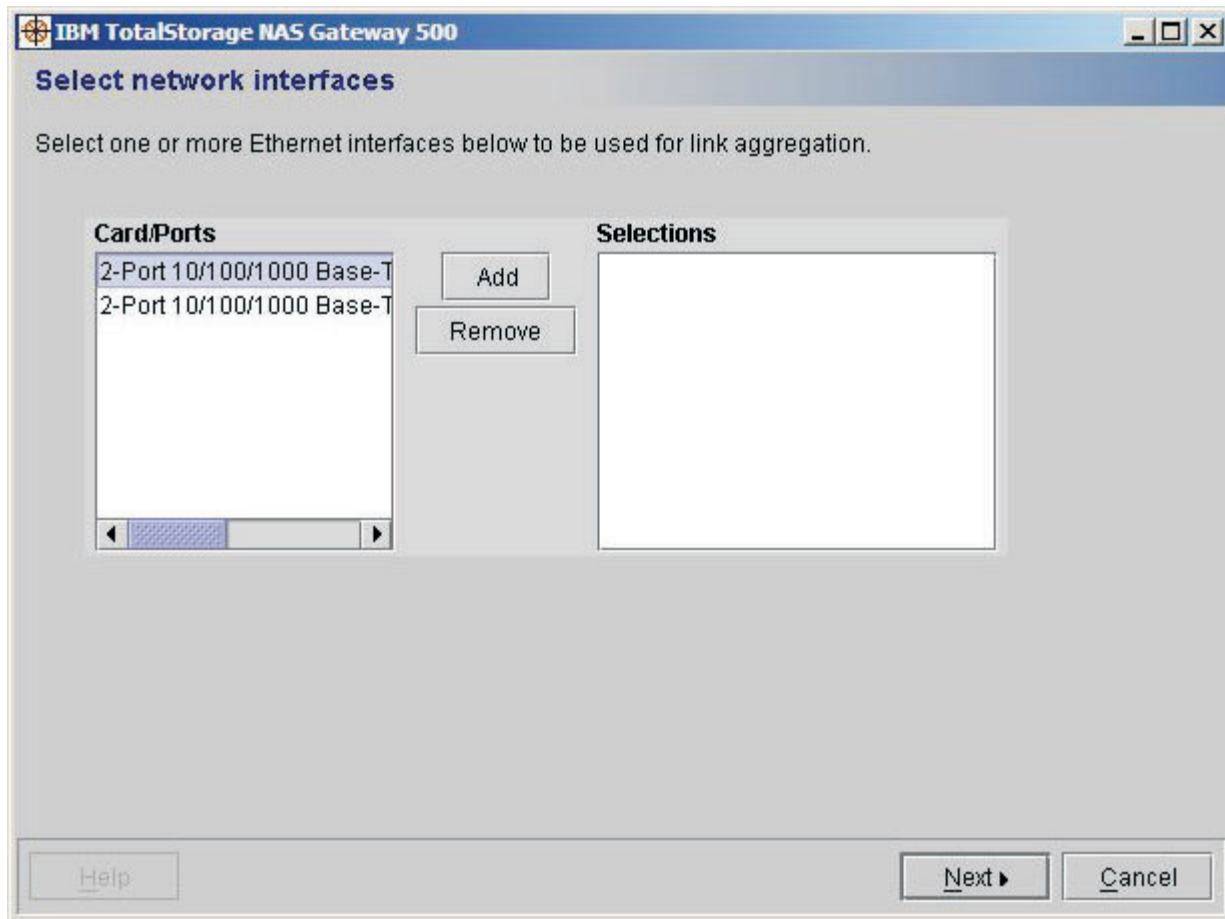


Figure 37. Select network interfaces

2. You are then asked to set your link aggregation options:

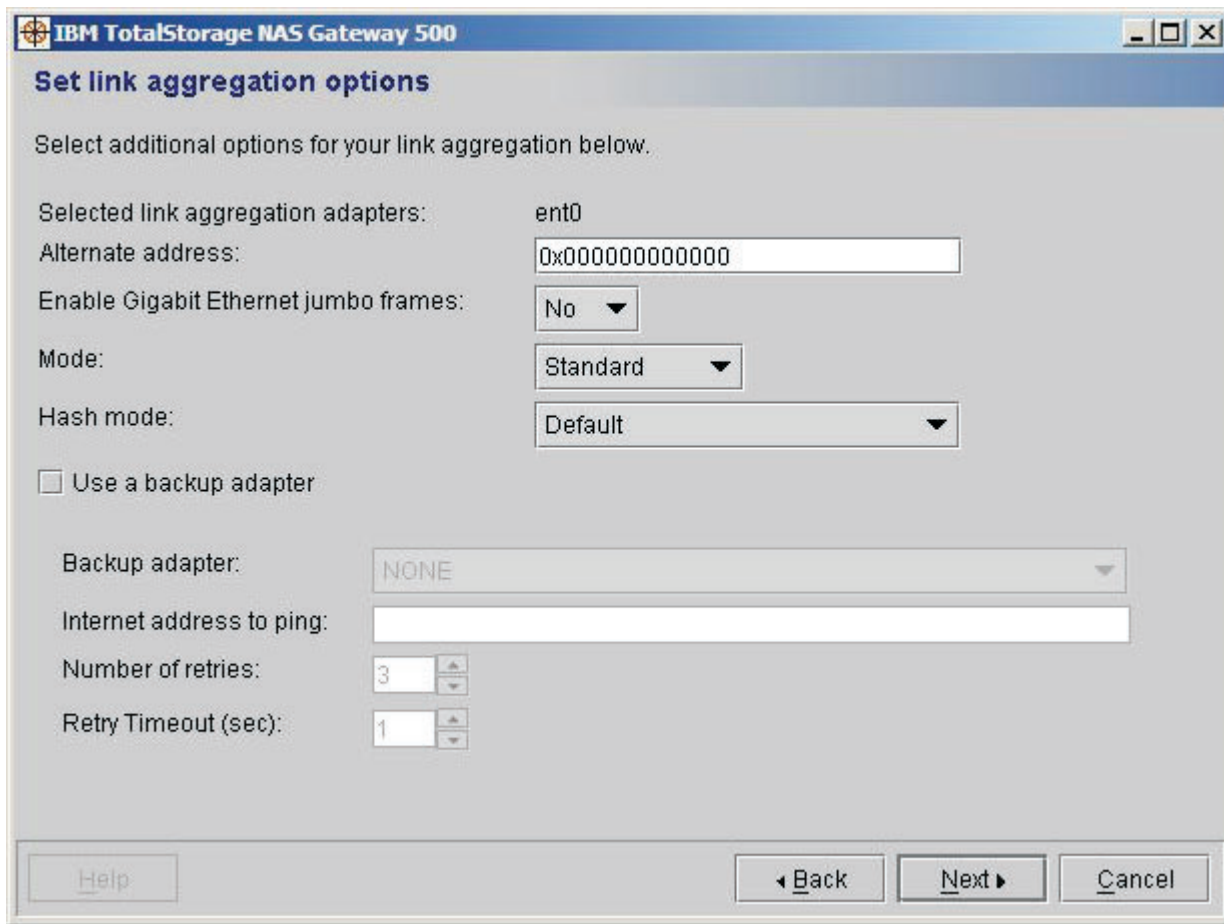


Figure 38. Set link aggregation options

Options include:

- **Alternate address:** The alternate hardware or MAC address used for the aggregation. All addresses are twelve-digit hexadecimal numbers preceded by *0x*. A default value of *0x* followed by 12 zeroes specifies that no alternate address should be used.
- **Enable Gigabit Ethernet jumbo frames:** This specifies whether Ethernet jumbo frames are enabled. If they are, then all adapter ports that are part of the link aggregation must support Ethernet jumbo frames.
- **Mode:** This specifies the type of link aggregation you are using. The default value is *standard*.

Valid values are:

- **standard:** standard EtherChannel is used. This means a hashing algorithm is used to ensure that all packets to a single destination are sent in order.
  - **round\_robin:** EtherChannel will alternate packets among all adapters, which may result in packets arriving out of order at their destination.
  - **8023ad:** This specifies that IEEE 802.3ad Link Aggregation is used.
- **Hash mode:** This specifies the hashing algorithm used to select the outgoing adapter, when standard or 8023ad modes are selected. The default value is *default*.

Valid values are:

- default: Hashing is done on the last byte of the IP address for IP traffic, and on the MAC address for non-IP traffic.
- src\_port: Hashing is done on the source TCP/UDP port value.
- dst\_port: Hashing is done on the destination TCP/UDP port value.
- src\_dst\_port: Both the source and destination TCP/UDP port value is used for hashing.
- Backup adapter parameter: This specifies which Ethernet device to use as a backup in case all ports in the link aggregation device fail. The backup adapter must use a separate switch and physical network cabling from the active adapters in the link aggregation to avoid a single point of failure.

**Note:** If a backup adapter is specified, and the link aggregation successfully fails over to the backup adapter, clustering will not perform a failover because the link aggregation will still be functional.

- Internet Address to ping: This specifies which IP address to ping to allow detection of the network failure and to trigger failover to the backup adapter. This option generates some network traffic, which slightly increases the network load. This option is useful only if a backup adapter is specified.
- Number of retries: The number of times ping is retried before the link aggregation determines that all ports are unstable, and fails over to the backup adapter. This option is enabled only when the backup adapter and the IP address to ping are specified.
- Retry timeout : The frequency (in seconds) with which ping is retried when determining the link aggregation status. This option is enabled only when a backup adapter and an IP address to ping are specified.

After making your selections, click **Next**.

3. You have completed the Link Aggregation Wizard. Click **Finish** to exit the wizard, or **Configure Another Link Aggregation** to configure another link aggregation.

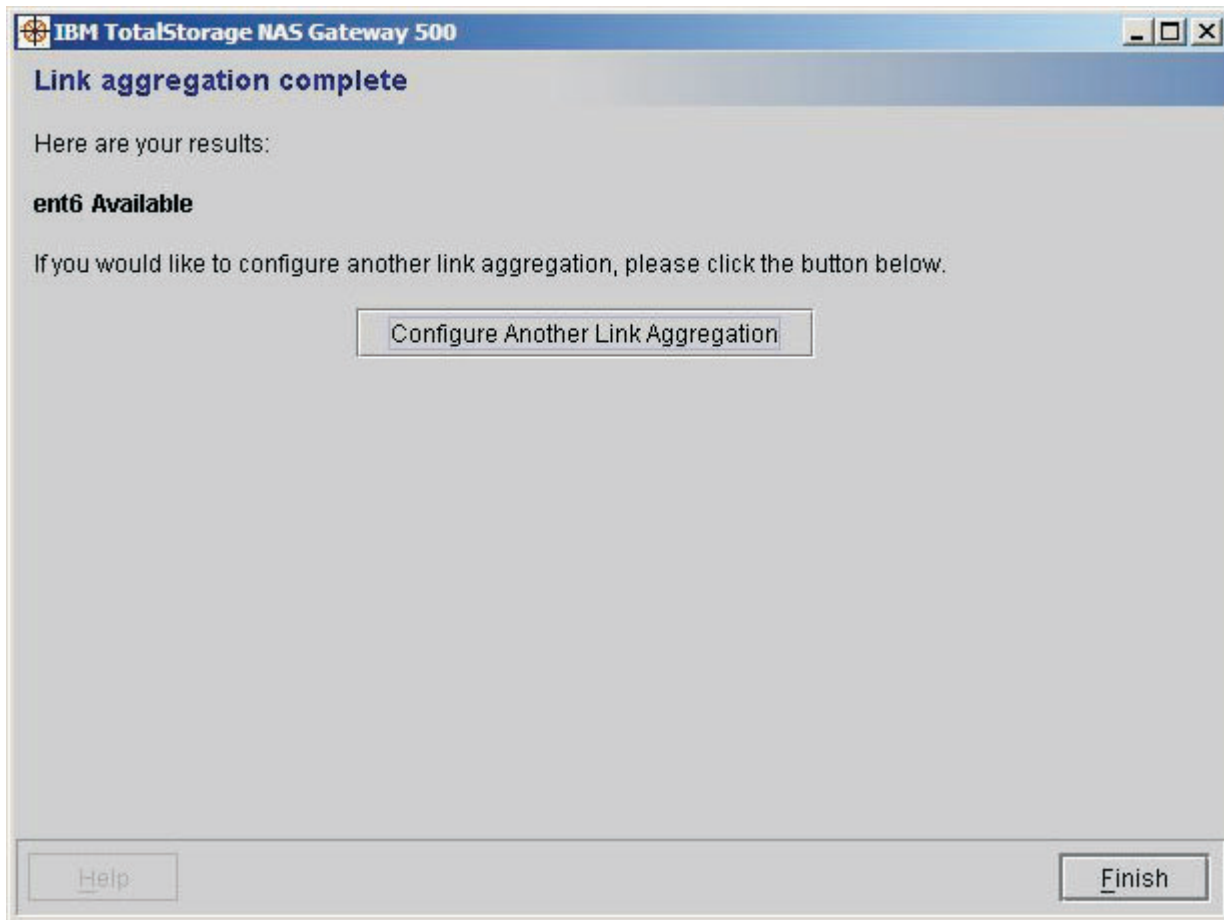


Figure 39. Link aggregation complete

## Chapter 15. Running wizards after initial configuration

**Note:** The wizards are best viewed with a screen resolution of 1024x768. Use of other resolutions results in the truncation of some data display fields.

This chapter describes the steps necessary to enter into specific wizards after you have completed initial configuration. There might be cases where there is a requirement to run a wizard after initial configuration, such as the addition of additional hard disks to an external disk storage system that is attached to the NAS Gateway 500. To reenter any of these wizards, start the Web-based System Manager Remote Client and click the + (plus sign) next to NAS Management in the left pane to expand the tree.

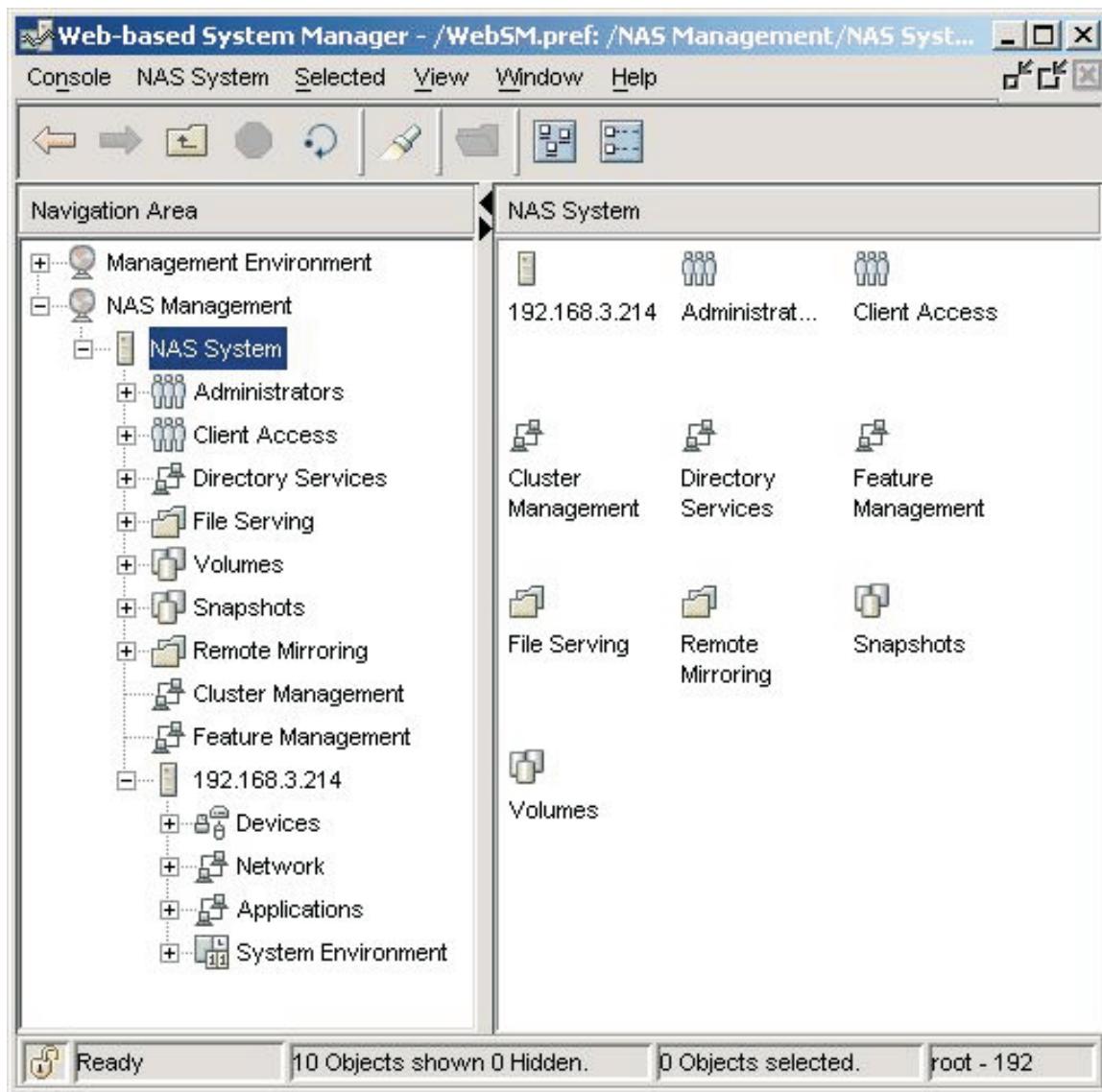


Figure 40. Web-based System Manager panel

---

## Feature Management Wizard

The Feature Management Wizard allows you to add or remove features. If you are adding features, the appropriate wizard will be launched upon exit of this wizard. To access this wizard:

1. In the left pane, click **Feature Management**.
2. To add or remove features:
  - In the right pane, click **Add Features** to add features.
  - In the right pane, click **Remove Features** to remove features.

---

## Remote Mirroring Wizard

To run the Remote Mirroring Wizard:

1. In the left pane, click the + (plus sign) next to **Remote Mirroring**.
2. In the left pane, click **Overview and Tasks**.
3. In the right pane, click the **Remote Mirror Wizard**.

---

## Link Aggregation Wizard

To run the Link Aggregation Wizard:

1. In the left pane, click the + (plus sign) next to the node.
2. In the left pane, click the + (plus sign) next to **Devices**.
3. In the left pane, click the + (plus sign) next to **Communication**.
4. In the left pane, click **Overview and Tasks**.
5. In the right pane, click **Create Link Aggregation**.

---

## Static Routes Wizard

To run the Static Routes Wizard:

1. In the left pane, click the + (plus sign) next to the node.
2. In the left pane, click the + (plus sign) next to **Network**.
3. In the left pane, click **Overview and Tasks**.
4. In the right pane, click **Static Routes Wizard**.

---

## Cluster Wizard

The Cluster Wizard can be run to configure a newly added cluster feature or modify an existing one:

1. In the left pane, click **Cluster Management**.
2. In the right pane, click **Configure Cluster**.

---

## CIFS Wizard

The CIFS Wizard can be run to configure a newly added CIFS feature or modify an existing one.

1. In the left pane, click the + (plus sign) next to File Serving.
2. In the left pane, click the + (plus sign) next to CIFS.
3. In the left pane, click **Overview and Tasks**.
4. In the right pane, click **CIFS Wizard**.

---

## Volume Wizard

If you want to add additional volumes after completing initial configuration, start the Volume Wizard as follows:

1. In the left pane, click the **+** (plus sign) next to Volumes.
2. In the left pane, click **Overview and Tasks**.
3. In the right pane, click **Create a NAS Volume**.

---

## NAS Administrator Wizard

If you want to add additional NAS administrators after completing initial configuration, start the NAS Administrator Wizard as follows:

1. In the left pane, click the **+** (plus sign) next to Administrators.
2. In the left pane, click **Overview and Tasks**.
3. In the right pane, click **Create a NAS Administrator**.

In a clustered environment, administrators that are added with this wizard are propagated to the remote node.

---

## File Access User Wizard

If you want to add additional file access users after completing initial configuration, start the File Access User Wizard as follows:

1. In the left pane, click the **+** (plus sign) next to Client Access.
2. In the left pane, click **Overview and Tasks**.
3. In the right pane, click **Manage Users**.

In a clustered environment, file access users that are added with this wizard are propagated to the remote node.





---

## Part 3. User interfaces

The NAS Gateway 500 provides three different simplified user interfaces for configuration and management:

- Command Line Interface (CLI)
- System Management Interface Tool (SMIT)
- Web-Based System Manager (WebSM)

The various tasks for day-to-day management are performed by a NAS Administrator from one or more of these user interfaces, and in many cases are available in all three user interfaces.

The task descriptions in Part 4, “Managing the NAS Gateway 500,” on page 87 typically describe at least one way to accomplish a task even though it might be possible to accomplish the same task using other user interfaces. See Appendix B, “Command shortcuts using SMIT fastpath and WebSM,” on page 259 for a list of the CLI commands and the associated SMIT and WebSM interface instructions.

The NAS Gateway 500 operates in headless mode. The user interfaces are typically accessed from another host machine connected to the NAS Gateway 500 using a network connection. For the command line and SMIT, you can use **telnet** or attach a console to serial port 1 to access these interfaces on the NAS Gateway 500. For WebSM, you use a graphics-capable machine with the WebSM client installed.

This section contains the following chapters:

- Chapter 16, “Command line interface,” on page 77 provides information about the CLI.
- Chapter 17, “Using System Management Interface Tool,” on page 79 describes how to use SMIT.
- Chapter 18, “Using WebSM after initial configuration,” on page 83 describes how to use WebSM.



---

## Chapter 16. Command line interface

**Note:** Before you use the CLI, the initial configuration of the NAS Gateway 500 as described in Part 2, “Initial configuration,” on page 11 must be completed.

The command line interface (CLI) allows NAS administration commands to be issued by administrators who prefer working at a command line.

Appendix B, “Command shortcuts using SMIT fastpath and WebSM,” on page 259 contains a list of the CLI commands and the associated SMIT and WebSM interface instructions.

To use the NAS CLI, log on to the NAS Gateway 500 with a NAS Administrator ID.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference*, SC30-4074, for a description of the individual commands and their syntax.



## Chapter 17. Using System Management Interface Tool

**Note:** Before you use the System Management Interface Tool (SMIT) interface, the initial configuration of the NAS Gateway 500 as described in Part 2, “Initial configuration,” on page 11 must be completed.

SMIT is an interface to a set of menus that allows you to select tasks to be performed. It includes additional panels to gather information and ultimately to form and execute a command. Tasks are typically grouped together based on the set of functions to be performed for objects such as administrators, applications, devices, and so on.

To use SMIT, log on to the NAS Gateway 500 with a NAS Administrator ID. Enter **smit** or **smitty** and press **Enter**. The NAS System Management panel is displayed:

```

                                     NAS System Management

Move cursor to desired item and press Enter.

Manage Administrators
Manage Applications
Manage Client Access
Manage Cluster
Manage Devices
Manage File Serving
Manage Network
Manage Security
Manage System
Manage NAS volumes, Remote Mirrors, and Snapshots

Using SMIT (information only)

NAS Overview (information only)

Esc+1=Help      Esc+2=Refresh   Esc+3=Cancel   Esc+8=Image
Esc+9=Shell     Esc+0=Exit     Enter=Do
```

Figure 41. NAS System Management panel

The NAS System Management panel gives you a selection of menus. You can navigate to an entry and press **Enter** to take you to a submenu or to one or more panels to gather input to build and execute a command. You do not need to remember the command syntax and, in some cases, you can make your selection from selection lists rather than having to enter values.

If you select any of the **Manage...** menus, you are presented with the appropriate NAS Administration tasks. For additional information about managing the NAS Gateway 500, see Part 4, “Managing the NAS Gateway 500,” on page 87.

If you select **Using SMIT**, general information is provided about using the SMIT interface. Review this information to help you work efficiently in the SMIT interface.

If you select **NAS Overview**, you find an overview of the tasks that you can perform using the NAS System Management menu. Review this information to help you identify where you should navigate to within the SMIT interface to perform a particular task.

SMIT also provides fastpaths (such as **smit nas\_admin** to access the Manage Administrators menu) to allow for direct navigation to the desired subset of SMIT functionality. Table 3 provides SMIT fastpaths for various *menus* within the SMIT interface:

*Table 3. SMIT menu fastpaths*

<b>SMIT menu</b>	<b>Fastpath</b>
Manage Administrators	nas_admin
Manage Applications	nas_apps
Backup and Recovery with Tivoli Storage Manager (TSM)	tsm
SAN Management with Tivoli SAN Manager	tsanm
Storage Resource Management with Tivoli Storage Resource Manager (TSRM)	tsrm
Network Management with Simple Network Management Protocol (SNMP)	snmp
Manage Client Access	nas_client
Manage Local File Access Users and Groups	file_user_local
Manage Directories for File Access Users and Groups	file_user_dirs
Manage NIS	nis
Manage NIS+	nis_plus
Manage LDAP	ldap
Manage Clustering	nas_cluster
Manage Devices	nas_devices
Disk	diskcfg
Communication	commodev
Link Aggregation	linkagg
Manage File Serving	nas_file
Manage FTP	ftp
Manage HTTP	http
Manage NFS	nfs
Manage CIFS	cifs
Manage Network	nas_network
Configure TCPIP	tcpip
Manage Security	nas_security
NFS and NIS Security	nfs_security
Manage System	nas_system
Backup and Recovery	backup
Boot and Shutdown	boot_shut
Date and Time	date_time
Problem Determination	problems
System Information	sys_info
Show Network Statistics	netstats
Manage Local Volumes, Snapshots, and Remote Volumes	nas_vols
Manage Local Volumes	localvols

Table 3. SMIT menu fastpaths (continued)

<b>SMIT menu</b>	<b>Fastpath</b>
Manage Snapshots	snapshots
Manage Remote Volumes	remotevols
Manage Remote Mirroring	remotemirror

See Appendix B, “Command shortcuts using SMIT fastpath and WebSM,” on page 259 for a list of the SMIT fastpaths for various commands within the SMIT interface.





---

## Chapter 18. Using WebSM after initial configuration

**Note:** Before you use this WebSM interface, the initial configuration of the NAS Gateway 500 as described in Part 2, “Initial configuration,” on page 11 must be completed.

WebSM is a client-server Java application that gives you a powerful mechanism to manage NAS Gateway 500 systems with a familiar Web browser-like interface. This WebSM graphical user interface enables you to access and manage remote NAS Gateway 500 systems.

**Note:** The WebSM interface provides a subset of the functionality that is available using the command line or SMIT.

The WebSM application can be executed both from root and NAS Administrator login. However, you should log in as a NAS administrator when you want to perform NAS administration tasks.

To begin a NAS administrator session, you must:

1. Launch the WebSM Remote Client from another host system in your environment that has the WebSM Remote Client installed.
2. Log in with a NAS administrator ID to the IP address of the NAS Gateway 500.
3. The NAS Management realm is displayed as shown in Figure 42 on page 84.

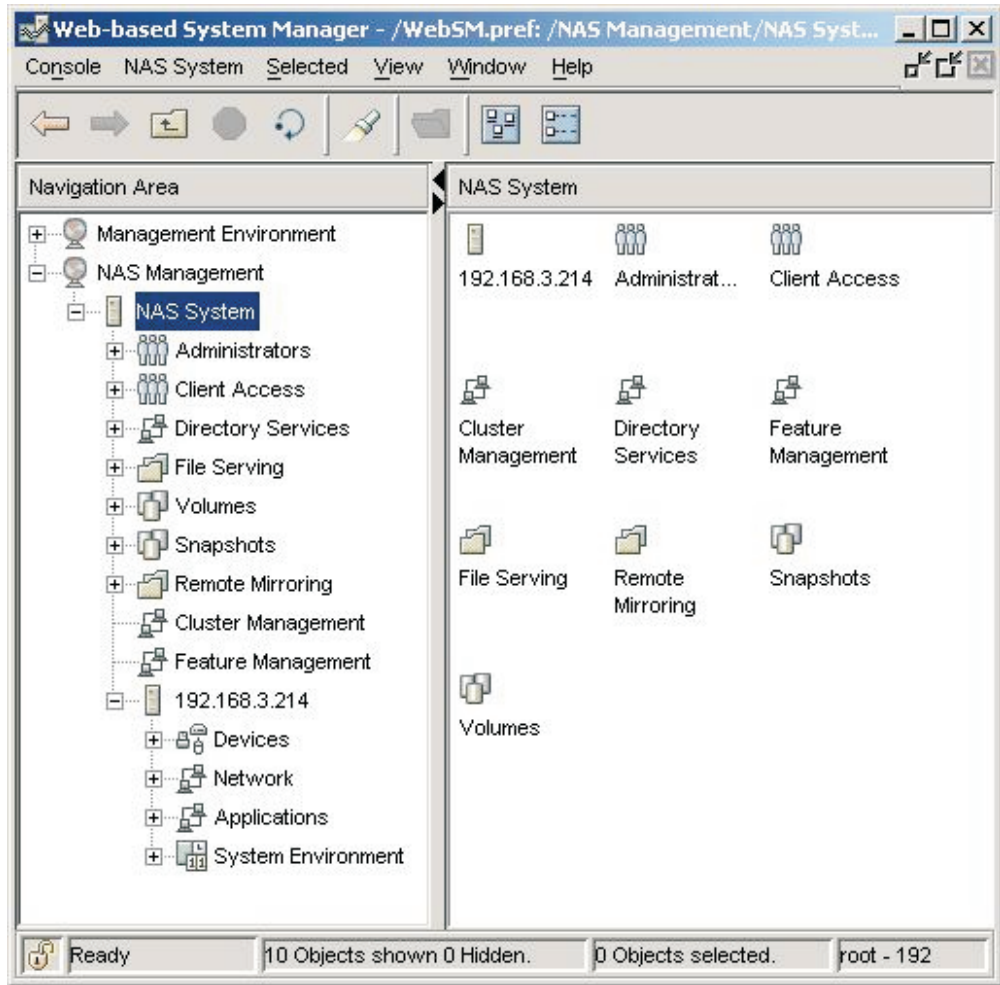


Figure 42. WebSM navigation and contents panels

The WebSM console interface provides a common launch point and navigation system for management of the NAS Gateway 500. The WebSM console follows the pervasive two-pane model in which a navigation area is presented in the left-hand pane and a contents area is presented in the right-hand pane. The navigation area presents the hierarchy of management tasks. The contents pane on the right displays results based on the object selected in the navigation panel.

See Appendix B, “Command shortcuts using SMIT fastpath and WebSM,” on page 259 for instructions on how to perform tasks using WebSM.

After the initial configuration is complete, you may want to install the WebSM Remote Client on other host machines in your environment to assist in management of one or more NAS Gateway 500 systems.

You can download the WebSM Remote Client by entering one of the following addresses in a Web browser.

If the desired language is English, the address is:

[http://HostAddress/NAS500WSMcli-en\\_US.html](http://HostAddress/NAS500WSMcli-en_US.html)

If the desired language is Japanese, the address is:

`http://HostAddress/NAS500WSMcli-ja_JP.html`

where *HostAddress* is the host name or IP address that is assigned to the NAS Gateway 500, or a specific node in the case of a cluster.



---

## Part 4. Managing the NAS Gateway 500

This section contains details of the day-to-day management tasks performed by the NAS administrator.

The following chapters provide an overview of the functionality of the NAS Gateway 500 and a description of many of the tasks that can be performed by the NAS administrator within each of these functional areas.

CIFS file serving, clustering, and Remote Mirroring are optional software features on the NAS Gateway 500 and must be ordered and enabled on the product before they can be used. Any references to these three features in this section assume that these features are enabled on your NAS Gateway 500.

**Note:** The task descriptions assume that you are logged in to the NAS Gateway 500 system as a NAS administrator.

This section contains the following chapters:

- Chapter 19, “NAS administrator common tasks,” on page 89 lists common tasks that are typically performed by the NAS administrator.
- Chapter 20, “Managing administrators,” on page 91 describes how to manage NAS administrator IDs.
- Chapter 21, “Managing applications,” on page 93 describes managing preinstalled applications to assist you with various management tasks.
- Chapter 22, “Managing client access,” on page 101 describes defining file access users.
- Chapter 23, “Managing clustered systems,” on page 109 describes managing clustered systems.
- Chapter 24, “Managing devices,” on page 119 describes managing the storage disks attached to your IBM TotalStorage NAS Gateway 500 system.
- Chapter 25, “Managing file serving,” on page 125 describes serving files using FTP, HTTP, NFS, and CIFS.
- Chapter 26, “Managing networking,” on page 149 describes the basic configuration of network adapters and interfaces.
- Chapter 27, “Managing security,” on page 153 describes managing NFS and NIS security.
- Chapter 28, “Managing the system,” on page 157 describes system-related tasks, such as backup and recovery, boot and shutdown options, date and time settings, problem determination, and system information.
- Chapter 29, “Managing NAS volumes, Remote Mirrored systems, and snapshots,” on page 165 describes managing NAS volumes and snapshots, and remote mirrored volumes and remote mirrored snapshots.



---

## Chapter 19. NAS administrator common tasks

The following are some common tasks that you can perform in managing the NAS Gateway 500.

---

### Creating users

When you create a new user who can access the files being served by the NAS Gateway 500, consider the following:

- You can add the user as a local file access user for NFS and FTP access (see “Adding a local file access user” on page 101), or you can add the user to a directory (see “Directory Services” on page 104).
- You can add the user for access from Windows machines using CIFS (see “Creating a CIFS user” on page 145).

**Note:** When you create a local file access user, you can also specify that the local file access user be added as a CIFS user as well (see “Adding a local file access user” on page 101).

- You can add a password for the local file access user to allow access using HTTP (see “Managing HTTP users” on page 127).

---

### Creating NAS volumes

When you want to create a NAS volume for storage on which to share files from the NAS Gateway 500, consider the following:

- Have you configured your physical storage? If you have not already done so, you must first configure the physical storage in your external disk storage subsystem. This will be done from another host machine in your environment using the management application provided with your storage subsystem. Refer to the documentation that was provided with your storage subsystem for more information on configuring the physical storage that will serve as physical disks to the NAS Gateway 500 system.
- Have you made configuration changes in your external disk storage subsystem? For example, to make storage disks available to the NAS Gateway 500 system, you must configure the NAS Gateway 500 to recognize these disks and make them ready for use as a NAS volume (see “Configuring devices” on page 119).
- Is this a clustered system configured for remote mirroring? If so, then you must stop the cluster before creating new volumes. See “Disabling the cluster” on page 110.
- Do you want to define a NAS volume using one or more physical disks available to the NAS Gateway 500 system and, as an option, remotely mirror the NAS volume (see “Creating a NAS volume” on page 166)?
- Do you want to configure a schedule for periodic snapshots of the contents of the NAS volume as part of your data protection strategy (see “Configuring a snapshot schedule” on page 181)?
- Do you want to plan a backup strategy for the NAS volume using the preinstalled Tivoli Storage Manager application (see “Using Tivoli Storage Manager (TSM)” on page 93)?

**Note:** If you are not creating a new NAS volume, and you want to mirror, see “Creating a remotely mirrored NAS volume” on page 173.

---

## Protecting your system and data

When you develop a strategy for protecting your system and data on NAS volumes, consider the following:

- Do you want to periodically perform a backup of your NAS system?
- Do you want to periodically perform a backup of your configuration files including following changes to the configuration files (see “Backup configuration files” on page 157)?
- Do you want to create a snapshot of a NAS volume (see “Creating a snapshot” on page 178) or configure a schedule for periodic snapshots of the contents of NAS volumes (see “Configuring a snapshot schedule” on page 181)?
- Do you want to plan a backup strategy for NAS volumes using the preinstalled Tivoli Storage Manager application (see “Using Tivoli Storage Manager (TSM)” on page 93)?



---

## Chapter 20. Managing administrators

A NAS administrator is a user who is responsible for the day-to-day administration of the NAS Gateway 500. One or more NAS administrators can be defined during initial configuration. The NAS administrator has a user name and a password. When the NAS administrator logs in to use the CLI or SMIT, the administrator is placed in a restricted shell. The restricted shell has a simplified set of commands and SMIT functions to assist in the management of the product. When the NAS administrator logs in to WebSM, the administrator is presented with a simplified NAS management interface to assist in the management of the product.

---

### Tasks used to manage administrators

You can use the SMIT fastpath **smit nas\_admin** to obtain the menu for Managing Administrators. Tasks in this menu are:

- “Adding a new administrator”
- “Changing an administrator’s password”
- “Showing the characteristics of an administrator” on page 92
- “List of all the administrators” on page 92

**Note:** Only the root user can remove a NAS administrator from the system.

### Adding a new administrator

You can add an administrator to allow other individuals to assist with management activities.

**Note:** After creating a NAS administrator, you need to create a password for the NAS administrator. See “Changing an administrator’s password.”

#### SMIT fastpath

You can use the SMIT fastpath **smit mknasadm** to add a new administrator. You must specify at least the user name for the NAS administrator. You can optionally specify other attributes.

#### WebSM

To add a new administrator using WebSM, navigate to: **NAS Management**→**NAS System**→**Administrators**→**Overview and Tasks**→**Create a NAS administrator**→**click ADD**. Enter the administrator User name and Full name and then click **OK**. Then enter the new password, confirm the password and click **OK**.

### Changing an administrator’s password

You must set the initial password for a NAS administrator after you create a NAS administrator. NAS administrators can also change their own password.

**Note:** A NAS administrator cannot change the password of another NAS administrator after setting the initial password. The root user can change the password for any NAS administrator.

#### SMIT fastpath

You can use the SMIT fastpath **smit passwdadm** to change an administrator’s password.

### **WebSM**

To change an administrator's password using WebSM, navigate to: **NAS Management**→**NAS System**→**Administrators**→**All NAS Administrators**→(right-click the administrator name)→**Change Password**.

## **Showing the characteristics of an administrator**

You can display the set of characteristics for a NAS administrator. These are the values that were specified when the NAS administrator user was created.

**Note:** A NAS administrator cannot change the characteristics for a NAS administrator.

### **SMIT fastpath**

Use the SMIT fastpath **smit lsnasadm** to display the characteristics for a NAS administrator.

### **WebSM**

To show the characteristics of an administrator using WebSM, navigate to: **NAS Management**→**NAS System**→**Administrators**→**All NAS Administrators**→(right-click the administrator name)→**Properties**.

## **List of all the administrators**

You can display a list of all of the NAS administrators that have been defined on the system.

### **SMIT fastpath**

Use the SMIT fastpath **smit lsnasadm** to display the list of NAS administrators.

### **WebSM**

To list all administrators using WebSM, navigate to: **NAS Management**→**NAS System**→**Administrators**→**All NAS Administrators**.

---

## Chapter 21. Managing applications

The NAS Gateway 500 includes several preinstalled applications to assist you with various management tasks. These applications provide some form of agent or client functionality that allow the NAS Gateway 500 to integrate in your environment and interact with other management products that you may have installed on other hosts or management stations. You can perform configuration and management of these agents or clients to allow them to interact with your management products.

The included applications can be used for various system management tasks such as backup and recovery, SAN management, storage resource management, and network management.

Application functionality includes:

- Backup and Recovery with Tivoli Storage Manager (TSM) client and storage agent
- SAN Management with Tivoli SAN Manager agent
- Storage Resource Management with Tivoli Storage Resource Manager (TSRM) agent
- Network management with Simple Network Management Protocol (SNMP)

---

### Using Tivoli Storage Manager (TSM)

This section describes how to configure and use the preinstalled Tivoli Storage Manager (TSM) Backup/Archive client and how to set up the Tivoli Storage Manager agent for LAN-free operations. The TSM client is one part of a total enterprise backup and recovery solution. This application gives the NAS Gateway 500 owner the ability to back up and restore data from a separate TSM server.

### Configuring the TSM client

Before you can back up or restore data using TSM, you must configure the TSM client that is preinstalled on the NAS Gateway 500. To configure the TSM client, you need the following information:

- TSM server name
- TSM server TCP/IP address
- TSM server TCP/IP port
- TSM client node name
- TSM client password

For more information about TSM client version 5.2, refer to <http://publib.boulder.ibm.com/tividd/td/IBMTivoliStorageManagerClient5.2.html>.

#### SMIT fastpath

The SMIT menu fastpath command is **smit tsmcsetconfig**.

To use the SMIT interface, go to **SMIT→Manage Applications →Backup and Recovery with Tivoli Storage Manager (TSM)→Configure TSM Client**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

After the information is entered and saved, you can perform a TSM backup or restore the data.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**TSM** →**Configure TSM Client**→specify settings→**OK**.

## Backup

### SMIT fastpath

The SMIT menu fastpath command for incremental backup is **smit tsmcbackupi**.

The SMIT menu fastpath command for selective backup is **smit tsmcbackups**.

Go to **SMIT**→**Manage Applications** →**Backup and Recovery with Tivoli Storage Manager (TSM)**→**Backup using TSM**→**TSM Incremental Backup**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

Press **F4** to display a list of the NAS volumes available for backup (for example: /Vols/nasvol1). This input is passed to the TSM client for command line execution. The files then go to the TSM server for backed up data management. The migration of data to tape occurs within the TSM server definitions, outside of the NAS Gateway 500.

## WebSM

From the main WebSM panel, navigate to : **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**TSM**→**Backup Using TSM Client**→specify settings→**OK**.

## Restore

### SMIT fastpath

The SMIT menu fastpath command to restore volumes is **smit tsm\_recov**.

The SMIT menu fastpath command to restore files is **smit tsmcrestoref**.

Go to **SMIT**→**Manage Applications** →**Backup and Recovery with Tivoli Storage Manager (TSM)**→**Recover using TSM**→**TSM Restore Volume(s)**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

Additional TSM client-specific restore options include:

#### **-subdir=yes**

To restore all files in all subdirectories.

#### **-replace=all**

To restore all files without prompting.

These options can be added to the entry for restoring the file or volume. For example:

```
/Vols/nasvol2/ -subdir=yes -replace=all
```

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**TSM**→**Recover Using TSM Client**→specify settings→**OK**.

For more information about TSM server version 5.2, refer to <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html#S>.

## Configuring the TSM storage agent

The Tivoli Storage Manager (TSM) storage agent version 5.2.2 comes installed on the NAS Gateway 500 and has been disabled from starting on boot until configuration is performed. To configure the TSM storage agent:

1. Refer to chapters 2, 3, and 4 in the *Storage Agent User's Guide for AIX Version 5.2* at <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html#S> for information about the prerequisite work required to configure the TSM storage agent on the NAS Gateway 500.
2. Root access to the NAS Gateway 500 machine is required.
3. SAN paths to all devices are required for the TSM storage agent to work properly.
4. After the prerequisite work is completed, you need the following information to configure the TSM storage agent using the NAS Gateway 500 SMIT interface:
  - Storage agent name
  - Storage agent password
  - Storage agent TCP/IP address
  - TSM server name
  - TSM server password
  - TSM server TCP/IP address
  - TSM Server TCP/IP port

### SMIT fastpath

The SMIT menu fastpath command is **smit tsmasetconfig**.

To use the SMIT interface, go to **SMIT→Manage Applications →Backup and Recovery with Tivoli Storage Manager (TSM)→Configure TSM Storage Agent**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSM→Configure TSM Storage Agent→specify settings→OK**.

## Starting and stopping the TSM storage agent

After the information has been entered and saved, you can use SMIT to start or stop the TSM storage agent.

### SMIT fastpath

The SMIT menu fastpath command is **smit tsmasetstate**.

Go to **SMIT→Manage Applications →Backup and Recovery with Tivoli Storage Manager (TSM)→Start/Stop TSM Storage Agent**. Move the cursor to Entry Fields to enter or select values. Change the state to *Start* or to *Stop* and press **Enter** to start or stop the TSM storage agent process.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSM→Start or Stop TSM Storage Agent→specify settings→OK**.

## Showing or changing the boot state of the TSM storage agent

The default for TSM Storage Manager is *off* (not to start on boot). The Start / Stop TSM Storage Agent panel only starts and stops the storage agent process. If the NAS Administrator wants the process to start all the time, then the boot state of the TSM storage agent needs to be changed to *on*.

### SMIT fastpath

The SMIT menu fastpath command is **smit tsmasetboot**.

Go to **SMIT→Manage Applications →Backup and Recovery with Tivoli Storage Manager (TSM)→Show / Change Boot State of TSM Storage Agent**. Move the cursor to Entry Fields and change the Boot state to *on*. Press **Enter**. When the change is entered, the TSM storage agent process starts on boot. The TSM storage agent will need to be stopped before you can make configuration change.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSM→TSM Storage Agent Boot Option→specify settings→OK**.

---

## Using Tivoli Storage Area Network Manager (TSANM)

This section describes how to configure and use the Tivoli Storage Area Network Manager (TSANM) agent on the NAS Gateway 500. The TSANM agent collects SAN-related information for reporting to a TSANM server. Once this information is collected, analysis and action can be performed on your SAN.

Once the TSANM agent is running, it communicates with the TSANM server and reports SAN related information. All report creation and generation is performed on the TSANM server or manager admin client. Refer to the TSANM server documentation on how to manage your SAN. For more information, go to <http://publib.boulder.ibm.com/tividd/td/StorageAreaNetworkManager1.2.html>.

## Configuring Tivoli SAN Manager agent

You must gather the following information so the NAS Gateway 500 can interface with the TSANM server:

- TSANM server TCP/IP address
- TSANM server TCP/IP port
- TSANM agent TCP/IP port

### SMIT fastpath

The SMIT menu fastpath command is **smit tsanmasetconfig**.

To use the SMIT interface, go to **SMIT→Manage Applications→SAN Management with Tivoli SAN Manager→Configure SAN Manager Agent**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

After the configuration information is entered and saved, you must set the TSANM agent password.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSANM→Configure TSANM Agent→specify settings→OK**

## Setting the password for the Tivoli SAN Manager agent

You must gather the following information to set the TSANM server password:

- TSANM Manager ID (this is set at the server)
- TSANM Manager password
- Authorized Password (this is the password that allows the TSANM agent to communicate with the TSANM server).

### SMIT fastpath

The SMIT menu fastpath command is **smit tsanmasetpass**.

Go to **SMIT→Manage Applications→SAN Management with Tivoli SAN Manager→Set Password for SAN Manager Agent**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSANM→Configure TSANM Agent password→specify settings→OK**.

## Starting and stopping the Tivoli SAN Manager agent

### SMIT fastpath

The SMIT menu fastpath command is **smit tsanmasetstate**.

You can use SMIT to start and stop the Tivoli SAN Manager agent. Go to **SMIT→Manage Applications→SAN Management with Tivoli SAN Manager→Start / Stop Tivoli SAN Manager Agent**. Move the cursor to Entry Fields to enter or select values.

Change the state to *start* or *stop* and then press **Enter** to start or stop the Tivoli SAN Manager agent process.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSANM→Start or Stop TSANM Agent→specify settings→OK**.

## Showing or changing the boot state of the Tivoli SAN Manager agent

The default for Tivoli SAN Manager agent is *off* (not to start on boot). The Start / Stop Tivoli SAN Manager Agent panel only starts and stops the Tivoli SAN Manager agent process. If the NAS Administrator wants the process to start all the time, then the boot state of the Tivoli SAN Manager agent needs to be changed to *on*.

### SMIT fastpath

The SMIT menu fastpath command is **smit tsanmasetboot**.

Go to **SMIT→Manage Applications→SAN Management with Tivoli SAN Manager→Show / Change Boot State of Tivoli SAN Manager Agent**. Move the cursor to Entry Fields and change the Boot state to *on*. Press **Enter**. When the change is entered, the Tivoli SAN Manager agent process will start on boot.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSANM→TSANM Agent Boot Option→specify settings→OK**.

---

## Using Tivoli Storage Resource Manager (TSRM)

This section describes how to configure and use the Tivoli Storage Resource Manager (TSRM) agent on the NAS Gateway 500.

### Establishing quotas with TSRM

An active TSRM agent collects information about the users and system for reporting to a TSRM server. Once the information has been sent to the TSRM server, quotas can be activated for alerts on certain users or groups.

After the TSRM agent is running, it communicates with the TSRM server and starts reporting storage and user-related information. All report creation and generation is performed on the TSRM server or manager administration client. For information about the Tivoli Storage Resource Manager server refer to <http://publib.boulder.ibm.com/tividd/td/tdprodlist.html#S>.

### Configuring the TSRM agent

You must gather the following information so that the NAS Gateway 500 can interface with the TSRM server:

- TSRM server TCP/IP address
- TSRM server TCP/IP port
- TSRM agent TCP/IP port

#### SMIT fastpath

The SMIT menu fastpath command is **smit tsrmasetconfig**.

To use the SMIT interface, go to **SMIT→Manage Applications→Storage Resource Management with Tivoli Storage Resource Manager→**. Move the cursor to Entry Fields to enter or select values. Press **Enter**.

#### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSRM→Configure TSRM Agent→**specify settings→**OK**.

### Starting and stopping TSRM agent

You can use SMIT to start and stop the TSRM agent.

#### SMIT fastpath

The SMIT menu fastpath command is **smit tsrmasetstate**.

Go to **SMIT→Manage Applications→ Storage Resource Management with Tivoli Storage Resource Manager (TSRM)→Start / Stop TSRM Agent**. Move the cursor to Entry Fields to enter or select values. Change the state to start or stop and press **Enter** to start or stop the TSRM agent process.

#### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSRM→Start or Stop TSRM Agent→**specify settings→**OK**.



## Showing or changing the boot state of the TSRM agent

The default for TSRM agent is *off* (not to start on boot). The Start / Stop TSRM Agent panel only starts and stops the TSRM agent process. If the NAS Administrator wants the process to start all the time, then the boot state of the TSRM agent needs to be changed to *on*.

### SMIT fastpath

The SMIT menu fastpath command is **smit tsrmasetboot**.

Go to **SMIT→Manage Applications→Storage Resource Management with Tivoli Storage Resource Manager (TSRM)→Show / Change Boot State of Tivoli SAN Manager Agent**. Move the cursor to Entry Fields and change the Boot state to *on*. Press **Enter**. When the change is entered the TSRM agent process starts on boot.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→TSRM→TSRM Agent Boot Option→specify settings→OK**.

---

## Using Simple Network Management Protocol (SNMP)

The NAS Gateway 500 includes an SNMP agent that can be used to obtain the values of Management Information Base (MIB) variables. A set of functions allows you to interact with the SNMP agent from the NAS Gateway 500 user interfaces to obtain these values using standard conventions.

You can use SMIT and select **Manage Applications** and then select **Network Management with Simple Network Management Protocol (SNMP)** or you can use the SMIT fastpath **smit snmp** to obtain the menu for SNMP tasks. The functions that you can perform include:

- “Getting SNMP information”
- “Setting SNMP information” on page 100
- “Dumping SNMP information” on page 100
- “Starting SNMP” on page 100
- “Stopping SNMP” on page 100

You can also interact with the SNMP agent from other higher-level management applications you may have in your environment for network or systems management.

## Getting SNMP information

You can get information about the NAS Gateway 500 using the SNMP agent provided within the NAS Gateway 500. You should be familiar with the particular MIB from which you want to obtain values and know either the text or numeric name of the specific variable whose value you want to read.

### SMIT fastpath

The SMIT fastpath command to read the value of a given MIB variable is **smit snmpinfo\_get**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Get SNMP Information→specify settings→OK**.

## Setting SNMP information

In some cases it is possible to set the value of the MIB variables. You should be familiar with the particular MIB for which you want to set values and know either the text or numeric name of the specific variable whose value you want to set as well as the instance of the variable. Note that only a subset of the variables in a MIB are writable.

### SMIT fastpath

The SMIT fastpath command to set the value of a given MIB variable is **smit snmpinfo\_set**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**SNMP**→**Set SNMP Information**→specify settings→**OK**.

## Dumping SNMP information

You can read the values of variables in an entire MIB tree for the SNMP agent to identify all of the variables that are supported. You can optionally specify a group such as system, interfaces, TCP, and so on from the MIB to subset the values returned.

### SMIT fastpath

The SMIT fastpath command to dump the values from the MIB tree is **smit snmpinfo\_dump**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**SNMP**→**Dump SNMP Information**→specify settings→**OK**.

## Starting SNMP

The SNMP agent is a daemon or background process that must be started to handle requests for MIB values.

### SMIT fastpath

The SMIT fastpath command to start the SNMP agent is **smit stsnmpd**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**SNMP**→**Start SNMP Service**→.

## Stopping SNMP

To prevent requests for MIB values, you can stop the SNMP agent. When the SNMP agent is stopped you cannot get, set, or dump MIB variable values.

### SMIT fastpath

The SMIT menu fastpath command to stop the SNMP agent is **smit spsnmpd**.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Node (Server IP Address)**→**Applications**→**SNMP**→**Stop SNMP Service**→.

---

## Chapter 22. Managing client access

The NAS Gateway 500 supports a number of mechanisms for defining users to allow you to control access to files being served by the NAS Gateway 500.

The following sections will explain how you can define these file access users locally on the NAS Gateway 500 or in a separate directory service.

- For managing local file access users, see “Local file access users.”
- For managing file access users using a directory service, see “Directory Services” on page 104.

---

### Local file access users

You can define file access users locally on the NAS Gateway 500 if you are not using a directory service such as NIS, NIS+, or LDAP. The local file access users that you define are used in authentication for access to files served by the NAS Gateway 500 using NFS or FTP.

See “Common Internet File System” on page 137 for information about managing user access to files served by the NAS Gateway 500 using CIFS.

See “HTTP” on page 126 for information about managing access to files served by the NAS Gateway 500 using HTTP.

Local file access users might have been defined during the initial configuration of the product. A local file access user has a user name, a password, primary and secondary groups, a home directory and other characteristics. During initial configuration, local file access users are created with an ID and password, using the standard default values for the other attributes.

**Note:** A local file access user cannot log in to the NAS Gateway 500.

You can use the SMIT fastpath **smit file\_user\_local** to obtain the menu for Manage Local File Access Users and Groups. Using Manage Local File Access Users and Groups you can perform the following tasks:

- “Adding a local file access user”
- “Changing a local file access user’s password” on page 102
- “Changing or showing characteristics of a local file access user” on page 102
- “Removing a local file access user” on page 102
- “Listing local file access users” on page 103
- “Setting or changing a CIFS user’s password” on page 103
- “Adding a group” on page 103
- “Changing or showing characteristics of a group” on page 103
- “Removing a group” on page 103
- “Listing all groups” on page 104

### Adding a local file access user

You can add a local file access user to allow access to files served by the NAS Gateway 500 using NFS and FTP.

**Note:** After creating a local file access user, you will need to create a password for the local file access user. See “Changing a local file access user’s password.”

### **SMIT fastpath**

You can use the SMIT fastpath **smit mknasuser** to add a local file access user. You must specify at least the user name for the local file access user. You can optionally specify other attributes such as user information to help identify the user which is free-format text information (name, department, and so on). Although CIFS access is managed separately from the local file access for NFS and FTP, you can also specify to add the local file access user as a CIFS user.

### **WebSM**

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**Overview and Tasks**→**Create a new user**.

## **Changing a local file access user’s password**

You must set the initial password for a local file access user after you create a local file access user.

### **SMIT fastpath**

You can use the SMIT fastpath **smit passwduser** to change a local file access user’s password.

### **WebSM**

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Users**→(right-click a user)→**Change password**.

## **Changing or showing characteristics of a local file access user**

The characteristics for an existing local file access user can be displayed. You can optionally change some of these characteristics, such as the free-format user information or the groups to which the local file access user belongs.

### **SMIT fastpath**

You can use the SMIT fastpath **smit chnasuser** to show or change the characteristics of a local file access user.

### **WebSM**

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Users**→(right-click a user)→**Properties**.

## **Removing a local file access user**

Removing a local file access user deletes the local file access user’s id from the NAS Gateway 500, but does not remove the home directory or files created by the local file access user.

### **SMIT fastpath**

You can use the SMIT fastpath **smit rmnasuser** to remove a local file access user.

### **WebSM**

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**Overview and Tasks**→**Delete a user**.

## Listing local file access users

You can obtain a list of all the local file access users that have previously been defined on the NAS Gateway 500.

### SMIT fastpath

You can use the SMIT fastpath **smit lsnasuser** to list all local file access users.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Users**.

## Setting or changing a CIFS user's password

You can set or modify the password of a CIFS user.

### SMIT fastpath

Use the SMIT fastpath **smit file\_user\_local**. Then select **Set / Change a CIFS User's Password**.

## Adding a group

You can create a group of local file access users.

### SMIT fastpath

You can use the SMIT fastpath **smit mkgroup** to create a group of local file access users.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**Overview and Tasks**→**Create a new group**.

## Changing or showing characteristics of a group

You can display the characteristics for a group of file access users. You can also add local file access users to a group or remove local file access users from a group.

### SMIT fastpath

You can use the SMIT fastpath **smit chgroup** to display or change the characteristics of a group of local file access users.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Groups**→**(right-click a group)**→**Properties**.

## Removing a group

A group of local file access users can be removed. The group is removed from the system. However any local file access users that are members of the group are unaffected. Removing the group from the system does not remove the local file access users that are members of the group.

### SMIT fastpath

You can use the SMIT fastpath **smit rmgroup** to remove a group of local file access users.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Groups**→(right-click a group)→**Delete**.

## Listing all groups

You can display a list of all of the groups of local file access users that have been defined on the system.

### SMIT fastpath

You can use the SMIT fastpath **smit lsgroup** to display the list of groups of local file access users.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Client Access**→**All Groups**.

---

## Directory Services

The NAS Gateway 500 can be configured to use a directory service to manage NAS file access users, rather than managing them locally. This reduces the administrative effort required to keep your network users synchronized. The NAS Gateway 500 contains clients for three directory services: NIS, NIS+ and LDAP. When configured as a directory service client, users from the directory service are treated in the same manner as local NAS file access users.

**Note:** The NIS and NIS+ clients are mutually exclusive.

This section discusses the following NIS tasks:

- “Configuring the NAS Gateway 500 as a NIS client” on page 105
- “Changing or showing characteristics of the client configuration” on page 105
- “Changing the NIS domain name of this host” on page 106
- “Removing NIS client configuration” on page 106

The following tasks are NIS Server Administrator tasks. The SMIT menu fastpath is **smit nis**.

For detailed information about these tasks, refer to the *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*.

- Identifying the NIS server
- Configuring binding the client to the server
- Binding the client to a specific server
- Adding or deleting an Internet address to search for a NIS connection
- Showing the NIS map
- Showing values in the NIS map
- Showing the order number of the NIS map
- Setting or Changing the network password in NIS

The following tasks are NIS+ tasks:

- “Initializing the system for a NIS+ client” on page 106
- “Configuring the NAS Gateway 500 as a NIS+ client” on page 106
- “Removing NIS+ client configuration” on page 107

- “NIS+ credential administration” on page 107

The following tasks are NIS+ Server administrator tasks. The SMIT menu fastpath is **smit nis\_plus**.

For detailed information about these tasks, refer to the *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*.

- Starting and stopping the NIS+ daemon
- Displaying default values currently active in namespace
- Showing the state of the NIS+ Namespace
- Changing Time to Live values of objects or entries
- Listing contents of the NIS+ directory
- Displaying contents of NIS+ table
- Showing values in the NIS+ tables
- Searching the NIS+ tables

The following tasks are LDAP tasks:

- “Configuring the NAS Gateway 500 as an LDAP client” on page 107
- “Removing LDAP client configuration” on page 108

## Configuring the NAS Gateway 500 as a NIS client

This section describes using NIS as the user registry for the NAS Gateway 500.

The NIS client can be configured using the Initial Configuration Wizard.

For more information about NIS, refer to the *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*.

A NAS administrator can configure the NAS Gateway 500 as a NIS client. Setting up the NIS client requires two steps, changing your NIS domain name and configuring the NIS client daemon. To change your NIS domain name, see “Changing the NIS domain name of this host” on page 106.

**Note:** The NIS domain name should not be confused with the domain name service (DNS) domain.

### SMIT fastpath

To configure the NIS client daemon on this NAS Gateway 500, the SMIT menu fastpath command is **smit mkclient**.

## Changing or showing characteristics of the client configuration

This section describes how to start the ypbind daemon, which allows this host to operate as a client. If there are no NIS servers on the networks directly connected to this NAS, the name of a NIS server must be specified instead of broadcasting for one.

### SMIT fastpath

The SMIT menu fastpath command is **smit chclient**.

## Changing the NIS domain name of this host

This section describes how to change the NIS domain name of the host. A domain is a logical group of clients and servers. All hosts (clients and servers) within a domain must have the same domain name.

**Note:** The NIS domain name should not be confused with the domain name service (DNS) domain.

### SMIT fastpath

The SMIT fastpath command is **smit chypdom**.

## Removing NIS client configuration

If you no longer want to use the NIS client on the NAS Gateway 500, a NAS administrator can remove the NIS client configuration.

### SMIT fastpath

The SMIT fastpath command is **smit rmyip**.

## Initializing the system for a NIS+ client

You initialize the NIS+ Client by any of the following ways:

### Cold-start

Using the cold-start file of another NIS+ client, preferably one from the same domain, is the most secure method of setting up an NIS+ client because it ensures that the client obtains its NIS+ information from a trusted server.

### Hostname

Initializing by the Hostname method is more secure than the broadcast method because it specifies the IP address of the trusted server, rather than relying on a server to identify itself. However, if a router exists between the client and the trusted server, it can intercept messages to the trusted IP address and route the messages to an untrusted server.

### Broadcast

Broadcast is the simplest but least secure method.

The key domain is the domain where root's credentials are stored. If you do not specify a value, then the system default domain is used.

Use the following method to initialize a system for a NIS+ client.

### SMIT fastpath

To initialize a system for a NIS+ client, use the SMIT fastpath **smit nisinit**.

## Configuring the NAS Gateway 500 as a NIS+ client

This section describes using NIS+ as the user registry for the NAS Gateway 500.

For more information on NIS+, refer to the *AIX 5L Version 5.2 Network Information Services (NIS and NIS+) Guide*.

A NAS administrator can configure the NAS Gateway 500 as a NIS+ client. Before you configure the NIS+ client, ensure that the DES credentials have been created for each node of your NAS Gateway 500. You must also know:

1. Your NIS+ domain name



2. The name and IP address of the NIS+ server
3. The network password for the machine

This information should be obtained from your network administrator.

**Note:** The NIS+ domain name should not be confused with the domain name service (DNS) domain.

The common fields are:

**Domain name of this NIS+ host**

Specifies the NIS+ domain you want to join (for example, wiz.com.).

**Hostname of NIS+ server**

Specifies the host name of the NIS+ server for your domain.

**IP address of NIS+ server**

Specifies the IP address of the NIS+ server.

You can take the default values for the rest of the fields. Enter **y** when asked if you want to continue, and then enter your network password at the prompt. When the NIS+ client configuration is complete, you must reboot your NAS Gateway 500.

**SMIT fastpath**

The SMIT fastpath command is **smit nisclient**.

## Removing NIS+ client configuration

If you no longer want to use the NIS+ client on the NAS Gateway 500, a NAS administrator can remove the NIS+ client configuration.

To remove the NIS+ client configuration:

1. Use the SMIT fastpath: **smit nis\_plus**.
2. Select **Remove NIS+ Client Configuration from this Host**.
3. Confirm your selection.

## NIS+ credential administration

The NAS administrator can add LOCAL credentials or DES credentials to the root domain, or remove credential information from this local domain.

**SMIT fastpath**

To administer NIS+ credentials, use the SMIT fastpath **smit nisp\_creds**.

## Configuring the NAS Gateway 500 as an LDAP client

This section describes using LDAP as the user registry for the NAS Gateway 500.

For more information on LDAP, refer to the section entitled “LDAP Exploitation of the Security Subsystem” in the *AIX 5L Version 5.2 Security Guide*.

A NAS administrator can configure the NAS Gateway 500 as a LDAP client. Before you begin, ensure that you know the administrative account name and password for your LDAP server. This information should be obtained from your network administrator.

The fields in the SMIT dialog are:

<b>Server List</b>	A comma-separated list of LDAP servers. You can specify the servers by host name or IP address.
<b>Server Administrator DN</b>	The distinguished name (DN) of the LDAP administrator account. It must match the one used for the server setup.
<b>Server Administrator Password</b>	The password for the server administrator.
<b>Base DN</b>	An optional field specifying the base distinguished name (DN) to search for users and groups. If this field is left empty, the entire LDAP database is searched.
<b>Server Port</b>	An optional field used to override the default port (389) used for communication with the LDAP server.

### **SMIT fastpath**

The SMIT menu fastpath command is **smit mksecldap**.

## **Removing LDAP client configuration**

If you no longer want to use the LDAP client on the NAS Gateway 500, a NAS administrator can remove the LDAP client configuration.

### **SMIT fastpath**

The SMIT menu fastpath command is **smit mksecldapu**.

---

## Chapter 23. Managing clustered systems

This section describes how to manage clustered systems, including geographic clusters.

**Attention:** Modifications to the geographic cluster topology (such as hosts and host names, networks and IP addresses) and modifications to mirroring settings (such as remote priority node and mirroring mode) are only allowed when the cluster is disabled on all nodes of the geographic cluster.

**Note:** Modifications to cluster configuration (whether geographic or not) can only be made through the WebSM wizards.

The following file system operations are not allowed when a geographic cluster is running:

- Creating, changing, or removing a volume
- Creating, changing, or removing a remotely mirrored volume
- Importing or exporting a volume
- Creating or removing an NFS Export
- Creating or removing a CIFS Export

---

### Tasks used to manage clusters

You can use the following tasks to manage clustered systems:

- “Enabling the cluster” on page 110
- “Disabling the cluster” on page 110
- “Verifying clusters” on page 110
- “Synchronizing the cluster” on page 111
- “Deleting the cluster” on page 111
- “Showing cluster server state” on page 111
- “Enabling a server in the cluster” on page 112
- “Disabling a server in cluster” on page 112
- “Moving cluster service to another adapter” on page 113
- “Showing volumes being served” on page 113
- “Relocating volumes” on page 113
- “Enabling a volume in the cluster” on page 114
- “Disabling a volume in the cluster” on page 114
- “Enabling a resource group in the cluster” on page 115
- “Disabling a resource group in the cluster” on page 115
- “Viewing the cluster log” on page 115
- “Displaying information about cluster interfaces” on page 116
- “Modifying the cluster” on page 116

The following sections describe how to modify site topology.

- “Adding a GeoPrimary network” on page 116
- “Deleting a GeoPrimary network” on page 116
- “Changing a host name in the geographic cluster” on page 117

- “Modifying a host’s mirroring settings” on page 117
- “Adding another host in the geographic cluster” on page 117
- “Deleting a host in the geographic cluster” on page 118

## Enabling the cluster

To enable the cluster (start cluster services) on all NAS Gateway 500s, choose one of the following methods.

### CLI command

At the command prompt, enter **clnasencluster**.

### SMIT fastpath

The SMIT fastpath command to enable clustering is **smit clnasencluster**.

### WebSM

To enable clustering from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Enable cluster**.

## Disabling the cluster

When a cluster is configured using the Initial Configuration Wizard, the cluster is automatically enabled (that is, cluster services are started). If for any reason (such as maintenance or adding remote volumes) the cluster needs to be disabled (stopped), use the following procedures.

**Attention:** It is important to know that while the cluster is disabled, the volumes are not available for client access. You can stop clustering on one NAS Gateway 500 and have volumes remain available on another NAS Gateway 500. To do this, you must relocate the volumes to the NAS Gateway 500 that will remain active, and then use the procedure to disable the cluster on a single node.

To disable the cluster (stop cluster services) on all NAS Gateway 500s, choose one of the following methods.

### CLI command

At the command prompt, enter **clnasdiscluster**.

### SMIT fastpath

The SMIT fastpath command to disable clustering is **smit clnasdiscluster**.

### WebSM

To disable clustering from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management** →**Disable cluster**.

## Verifying clusters

Use this task to verify that the cluster is properly configured and synchronized.

### CLI command

At the command prompt, enter **clnasisconfiged**.

### SMIT fastpath

The SMIT fastpath command is **smit clnasisconfiged**.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Verify cluster**.

## Synchronizing the cluster

The definition of the cluster must be the same on all nodes to insure proper operation. Although the NAS commands are designed to keep the cluster definitions the same, or synchronized, it is possible that the nodes could end up out of synchronization. If this occurs, you should manually synchronize the cluster. Synchronization should be done from the node on which the latest changes have been made, so that the latest definition of the cluster is propagated to the other node.

If Remote Mirroring is enabled, synchronization of the cluster is not permitted if the cluster is enabled (running) on any node.

### CLI command

At the command prompt, enter **clnassync**.

### SMIT fastpath

The SMIT fastpath command is **smit clnassync**.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Synchronize cluster**.

## Deleting the cluster

**Attention:** Deleting the cluster removes all IP address settings, volume definitions, NFS exports, and CIFS shares from the cluster definition. If the cluster is re-created, these would have to be restored to the cluster by importing volumes, re-exporting NFS shares, and so on.

If a geographic cluster is deleted, it can only be redefined if you are logged in to WebSM client as root and all nodes are on the default root password of password.

### CLI command

At the command prompt, enter **clnasdelcluster**.

### SMIT fastpath

The SMIT fastpath command is **smit clnasdelcluster**.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Delete cluster**.

## Showing cluster server state

The state of one or all nodes in the cluster are displayed as one of the following:

- Idle
- Unknown
- Unstable
- Stable
- Reconfiguring

- Error

The states of Idle and Stable are normal states for a cluster that is disabled and for a cluster that is properly up and running, respectively. States of Unknown, Unstable, and Reconfiguring are transitional states if the cluster is in the process of being enabled, disabled, or a change has been made that affects the cluster.

### CLI command

At the command prompt, enter **clnasnodestate -n *nodename*** to see the state of a single node, or **clnasnodestate** to see the state of all nodes.

### SMIT fastpath

The SMIT fastpath command is **smit clnasnodestate**. Press **Enter** to see the state of all nodes, or enter a node name.

### WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Show server state**.

## Enabling a server in the cluster

**Attention:** If one of the NAS Gateway 500s in the cluster has been disabled while actively serving volumes, the volumes are again available for client access after that NAS Gateway 500 is enabled back into the cluster. If the volumes have been manually relocated to the other NAS Gateway 500 prior to disabling that NAS Gateway 500, those volumes remain relocated until you manually move them back.

To enable clustering on one NAS Gateway 500, choose one of the following methods:

### CLI command

To enable clustering on one NAS Gateway 500, enter **clnasenode -n *hostname*** command, where *hostname* is the name of the host that you entered during initial configuration.

### SMIT fastpath

The SMIT fastpath command to enable clustering on one NAS Gateway 500 is **smit clnasenode**. Select the appropriate host.

### WebSM

To enable clustering on one NAS Gateway 500 from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management** →**Enable server**. Select the appropriate host.

## Disabling a server in cluster

When a cluster is configured using the Initial Configuration Wizard, the cluster is automatically enabled (that is, cluster services are started). If for any reason (such as maintenance or adding remote volumes) the cluster needs to be disabled (stopped), use the following procedures.

**Attention:** It is important to know that while the cluster is disabled, the volumes are not available for client access. You can stop clustering on one NAS Gateway 500 and have volumes remain available on another NAS Gateway 500. To do this, you must relocate the volumes to the NAS Gateway 500 that remains active, and then use the procedure to disable the cluster on a single node, or you can specify to fail over to another node by specifying the **-f** option of the command.

### CLI command

To disable clustering on one NAS Gateway 500, enter **clnasdisnode -n *hostname*** command, where *hostname* is the name of the host that you entered during initial configuration.

### SMIT fastpath

The SMIT fastpath command to disable clustering on all nodes is **smit clnasdisnode**.

### WebSM

To disable clustering on all NAS Gateway 500s from the main WebSM panel, navigate to: **NAS Management→NAS System→Cluster Management→Disable server**.

## Moving cluster service to another adapter

You might want to move a file serving IP address to a different boot adapter, for example, for maintenance or load-balancing purposes. You can see which file serving IP addresses are on which boot adapter by executing the command **ifconfig -a** on the appropriate node. A file serving IP address can only be moved to another boot adapter on the same node; it cannot be moved to another node.

### CLI command

At the command prompt, enter **clnasmvservice -v *file\_serving\_IP\_address* -b *target\_boot\_adapter\_IP\_address***.

### SMIT fastpath

The SMIT fastpath command is **smit clnasmvservice**. Enter the file serving IP address and the target boot adapter IP address.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Cluster Management→Move service**.

## Showing volumes being served

You can view the volumes that are assigned to a particular node, as well as what volumes are actively being served by which node. The node name, name of the group (*hostname\_Vols*) containing the volumes, and list of volumes are displayed.

### CLI command

At the command prompt, enter **clnasshowvol** to see which volumes are assigned to which node, or **clnasshowvol -a** to see what volumes are actively being served from which node. You can also use **-n *node name*** to only look at a particular node.

### SMIT fastpath

The SMIT fastpath command is **smit clnasshowvol**. Choose a node name to view only a single node, or select **no** in the Show Inactive Volumes field to see only those volumes actively being served.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Cluster Management→Show volumes being served**.

## Relocating volumes

You can move an entire group of volumes being served from one node to the other node, for example for maintenance or load-balancing purposes. This command is

not executed if the cluster is in the Unstable or Idle (disabled) state on the target node. If Remote Mirroring is enabled, volumes cannot be manually moved from one site to the other. See “Managing Remote Mirrored systems” on page 175.

### CLI command

At the command prompt, enter **clnasrelocate -g *group\_name* -n *target\_node\_name***.

### SMIT fastpath

The SMIT fastpath command is **smit clnasrelocate**. Select the group name and the target node name.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Cluster Management→Relocate volumes**.

## Enabling a volume in the cluster

**Note:** You must not use this command if the Remote Mirroring feature is enabled and the cluster is enabled (running) on any node. In order to remount a volume in this case, use the **mountvol** command with the -f option.

Enabling a volume in the cluster restores the definition of that volume to the specified group. If the cluster is running, the volume is automatically mounted.

### CLI command

At the command prompt, enter **clnasenvol *volume\_name* *group\_name***.

### SMIT fastpath

The SMIT fastpath command is **smit clnasenvol**. Select the appropriate volume and group name.

### WebSM

From the main WebSM panel, navigate to: **NAS Management→NAS System→Cluster Management→Enable Volumes**.

## Disabling a volume in the cluster

**Note:** You must not use this command if the Remote Mirroring feature is enabled and the cluster is enabled (running) on any node. In order to temporarily unmount a volume in this case, use the **unmountvol** command with the -f option.

Disabling a volume removes its definition from the cluster. If the cluster is running and the volume is mounted, the volume is automatically unmounted.

**Note:** Disabling a volume in the cluster should only be used as a temporary measure to unmount a volume. Disabling the volume does not remove the dependent NFS exports or CIFS shares from the cluster.

### CLI command

At the command prompt, enter **clnasdisvol *volume\_name***.

### SMIT fastpath

The SMIT fastpath command is **smit clnasdisvol**. Select the volume.



## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Disable volumes**.

## Enabling a resource group in the cluster

You can enable the specified resource group. Any volumes that are defined to the resource group are mounted and available.

If a node name is not specified, the group is enabled on the node on which the command is executed.

### CLI command

At the command prompt, enter `clnasengroup -g [-n node_name] resource_group_name`.

### SMIT fastpath

The SMIT fastpath command to disable clustering on all nodes is **smit clnasengroup**.

## WebSM

To disable clustering on all NAS Gateway 500s from the main WebSM panel, navigate to: **Cluster Management**→**Enable resource group** .

## Disabling a resource group in the cluster

You can disable the specified resource group. Any volumes that are defined to the resource group is unmounted and unavailable.

### CLI command

At the command prompt, enter `clnasdisgroup -g resource_group_name`.

### SMIT fastpath

The SMIT fastpath command to disable clustering on all nodes is **smit clnasdisgroup**.

## WebSM

To disable clustering on all NAS Gateway 500s from the main WebSM panel, navigate to: **Cluster Management**→**Disable resource group**.

## Viewing the cluster log

If problems occur in the cluster, you can view the cluster logs for problem determination.

### CLI command

At the command prompt, enter `clnasviewlog log_file_name`. If a log file name is not explicitly specified, the IBM NAS Gateway 500 cluster configuration `nascluster.log` file is displayed. You can view the names of valid log files using the **clnaslogfilenames** command.

### SMIT fastpath

The SMIT fastpath command is **smit clnasviewlog**. Select the log to view.

## WebSM

From the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**View log**.

## Displaying information about cluster interfaces

You can display information about the cluster topology such as the networks, network interfaces, and resource groups. Additionally, if the cluster is enabled (that is, running) on a node, it shows the state of the cluster, what network interfaces are up or down relative to the nodes, and it shows the state and location of the resource groups.

### CLI command

At the command prompt, enter `clnasshowcluster`.

### SMIT fastpath

The SMIT fastpath command to disable clustering on all nodes is **smit clnasshowcluster**.

### WebSM

To disable clustering on all NAS Gateway 500s from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Show configuration**.

## Modifying the cluster

In order to modify the topology of the cluster, such as to change a host name or add, delete, or change an IP address, you must execute the NAS Gateway 500 WebSM Cluster Wizard. From WebSM, navigate to: **NAS Management**→**NAS System**→**Cluster Management**→**Configure Cluster**. If any changes are made from the wizard, do not exit the wizard until after the synchronization step, or you should synchronize the cluster manually from the local node once all changes are made.

**Note:** If this is a geographic cluster, no changes are allowed if the cluster is enabled (running) on any node. Otherwise, changing the cluster name, a host name, or a boot adapter is not allowed if the cluster is enabled on either node.

## Adding a GeoPrimary network

To add an additional GeoPrimary network to an existing geographic cluster:

1. Start the Remote Mirroring Wizard from WebSM with **Remote Mirroring**→**Remote Mirroring Wizard**.
2. Click **Next** at the Site Topology screen to leave the topology unchanged.
3. Click **Next** to leave the first GeoPrimary network at the local site unchanged.
4. Click **More Mirroring Networks** to add additional networks.
5. When finished, click **Next** to finish the Remote Mirroring Wizard.
6. Continue through to the end of the Cluster Wizard and click **Synchronize**, or exit the Cluster Wizard and synchronize the cluster using the command line, SMIT or WebSM.

## Deleting a GeoPrimary network

To remove a GeoPrimary network from an existing geographic cluster:

1. Start the Remote Mirroring Wizard using the WebSM **Remote Mirroring**→**Remote Mirroring Wizard**.
2. Click **Next** at the Site Topology screen to leave the topology unchanged.
3. If you want to delete the first network, click **Delete This Network**. Otherwise, click **Next** and **More Mirroring Networks** until you reach the network you want to delete. Then, click **Delete This Network**.

4. When finished, click **Next** to finish the Remote Mirroring Wizard.
5. Continue through to the end of the Cluster Wizard and click **Synchronize**, or exit the Cluster Wizard and synchronize the cluster using the command line, SMIT or WebSM.

## Changing a host name in the geographic cluster

To change the name of a host in the geographic cluster:

1. Start the Remote Mirroring Wizard from the WebSM **Remote Mirroring**→**Remote Mirroring Wizard**.
2. Click **Next** at the Site Topology screen to leave the topology unchanged. Or, if you want to change a host name at the local site, make the change and click **Next**.
3. If a host name at the remote site is to be changed, make the change and click **Next** to finish the Remote Mirroring Wizard.
4. Continue through to the end of the Cluster Wizard and click **Synchronize**, or exit the Cluster Wizard and synchronize the cluster using the command line, SMIT or WebSM.

## Modifying a host's mirroring settings

To modify a node's mirroring mode, file serving IP addresses, or remote priority node selection:

1. Start the Cluster Wizard from the WebSM **Cluster Management**→**Cluster Wizard**.
2. Click **Next** to advance to the node you want to change and make the changes.
3. Click **Next** to get to the Synchronization screen and click **Synchronize**.
4. When synchronization completes, click **Next** and **Finish** to exit the Cluster Wizard.

## Adding another host in the geographic cluster

**Important:** When adding another host to a site in a previously configured cluster, the following must be true:

- You must be logged in as the root user.
- The root password on the new hosts must be set to the default, which is "password".
- Integrated Ethernet port #2 on the hosts at the site or sites being modified must have a default IP address of 192.168.244.1.
- An Ethernet crossover cable must be connected between integrated ports #2 on both hosts.
- A NULL modem cable must be connected between serial port #3 on both hosts.

To add another host:

1. Start the Remote Mirroring Wizard from the WebSM **Remote Mirroring**→**Remote Mirroring Wizard**.
2. Change the Site Topology as appropriate to indicate the change from a single-host site to a dual-host site.
3. Click **Next**.
4. If adding a host at the local site, add the host and its IP address and port.
5. Click **Next**.

6. If adding a host at the remote site, add the host and its IP address and port.
7. For additional GeoPrimary networks, click **More Networks** and repeat the steps until done.
8. Click **Next** to finish the Remote Mirroring Wizard.
9. Proceed through the Cluster Wizard. When you are presented with a node screen for a new host, fill in all the appropriate information for that host.
10. Continue through to the end of the Cluster Wizard and click **Synchronize**.
11. When synchronization completes, click **Next** and **Finish** to exit the Cluster Wizard.

## Deleting a host in the geographic cluster

**Note:** Deleting a host removes all definitions for that host from the cluster, including all IP addresses and resource group. Any volumes being served by that host are removed from the cluster and are not accessible until added back to the cluster. All NFS export and CIFS share definitions for that host will also be removed, and must be redefined if the host is re-added.

To delete a host:

1. Start the Remote Mirroring Wizard from the WebSM **Remote Mirroring**→**Remote Mirroring Wizard**.
2. Change the Site Topology to indicate the change from dual-host site to single-host site.
3. Click **Next**.
4. Click **OK** at the Are You Sure? dialog box.
5. Select the host you want to delete and click **OK**.
6. Continue clicking **Next** to finish the Remote Mirroring Wizard.
7. Continue through to the end of the Cluster Wizard and click **Synchronize**, or exit the Cluster Wizard and synchronize the cluster using the command line, SMIT or WebSM.

---

## Chapter 24. Managing devices

**Note:** Before you can configure storage devices on the NAS Gateway 500, you must first configure and define the physical disks on your external disk storage system using the management application provided with your external storage subsystem. Refer to the documentation that comes with your storage. You cannot define the physical disks using the NAS Gateway 500; instead, you must use the management application on another host system. Once you have defined the physical disks, you can then configure the NAS Gateway 500 to use these physical disks that appear as storage disks to the NAS system software.

You can configure and manage the storage disks and communication devices attached to your IBM TotalStorage NAS Gateway 500 system. Configuring storage devices is necessary for ultimately creating NAS volumes from these disks to make the storage available to file access users. Configuring communication devices is an optional step that is necessary only if you plan to use link aggregation on your IBM TotalStorage NAS Gateway 500 system. The following sections describe some of the tasks that are available to NAS administrators.

---

### Tasks used to manage devices

Some of the tasks that are available to NAS administrators include:

- “Configuring devices”
- “Unconfiguring devices” on page 120

Tasks to display system configuration information include:

- “Displaying configured disks and attributes” on page 120
- “Displaying additional device-specific information” on page 121

Tasks to manage disks include:

- “Displaying installed devices and attributes” on page 121
- “Displaying the size of a local disk” on page 121
- “Removing volume information from a local physical disk” on page 122
- “Displaying the size of a remote disk” on page 122
- “Removing volume information from a remote physical disk” on page 123

Tasks to manage communication devices include:

- “Creating a link aggregation device” on page 123
- “Listing link aggregation devices” on page 123
- “Changing a link aggregation device” on page 124
- “Removing a link aggregation device” on page 124

**Note:** These instructions are provided for use by a NAS administrator. Root users should specify the full path (/opt/nas/bin) for the commands.

### Configuring devices

In order to ensure that the system recognizes all devices that have been attached, use the **cfgmgr** command. This command installs and configures all devices. In a clustered environment, this command installs and configures devices on all nodes.

### CLI command

At the command prompt, enter **cfgmgr**.

### SMIT fastpath

The SMIT menu fastpath command to configure a device is **smit cfgmgr**.

### WebSM

To configure a device using WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Overview and Tasks**→**Discover devices that were powered on after the last system restart**.

## Unconfiguring devices

You can move a device to a defined state so that the device is inaccessible. If necessary, you can delete the definition of the device from the system database. All child devices, if any, receive the same action.

### CLI command

At the command prompt, enter **rmdev**. You can choose to delete the definition of the device from the system's database or simply move the device to a defined state so that the data on the device is inaccessible.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for more information about the syntax for the **rmdev** command.

### SMIT fastpath

In SMIT, you can remove fibre-channel adapters, Ethernet adapters, and disks. The SMIT fastpath for this function is **smit rmdev**.

### WebSM

To unconfigure disks, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Disks**→. (**right-click the disk**) →**Take Offline (Make Defined)** or **Delete**.

## Displaying configured disks and attributes

You can verify that disks are configured and ready for use in a volume.

### CLI command

At the command prompt, enter the **lspvol** command. This displays the disks, the PVID, the volume it is a part of, as well as a description. To display attributes of a disk, such as the size, you can specify the disk.

For more information about displaying the size of a storage device, see "Displaying the size of a local disk" on page 121.

To view the configured disks on a system at the command prompt, enter **lspvol**. To view the attributes for **hdisk4** on the system, enter **lspvol hdisk4**.

### SMIT fastpath

The SMIT fastpath to view the configured disks is **smit lspvol**. To view the disk's attributes, use **smit lspvoldisk**.

### WebSM

To view the configured disks on a system, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Disks**→(**right-click a disk**)**Attributes**.

## Displaying the size of a local disk

To display the size of a local storage device, use the NAS command, **lspvol**, to view the attributes for the disk. The attributes for a storage device are displayed by specifying the name of the device.

For example, to determine the size of `hdisk2`:

```
$ lspvol hdisk2
```

An example of the output from executing this command is:

```
hdisk2          U0.1-P2-I3/Q1-W200200A0B80FD2A0-L1000000000000 1742    (700) Disk Array
Device
cache_method   fast_write      Write Caching method      False
ieee_volname   600A0B80000F8313000000203F547E2F IEEE Unique volume name   False
lun_id         0x0001000000000000 Logical Unit Number       False
prefetch_mult  1              Multiple of blocks to prefetch on read False
pvid           0000000068a79f550000000000000000 Physical volume identifier False
q_type         simple         Queuing Type               False
queue_depth    10            Queue Depth                 True
raid_level     5             RAID Level                  False
reassign_to    120           Reassign Timeout value     True
reserve_lock   yes           RESERVE device on open     True
rw_timeout     30            Read/Write Timeout value   True
scsi_id        0xef          SCSI ID                     False
size          20480        Size in Mbytes           False
write_cache    yes           Write Caching enabled      False
```

**Note:** The size information is in bold for emphasis.

## Displaying installed devices and attributes

To view the installed devices on a system, use the NAS command **lscfg**. By default, it displays the devices configured in the system. If you specify options, you can obtain information about a specific device, such as the World Wide Name (WWN) or the ROS level (firmware). See “Displaying additional device-specific information” for more information.

### CLI command

At the command prompt, enter the **lscfg** command.

This displays the devices in the system configuration. For example, to display additional information for a fibre-channel adapter, enter: **lscfg -vl fcs0**.

### SMIT fastpath

The SMIT fastpath to view the configured disks is **smit lscfg**.

### WebSM

To view the Vital Product Data (VPD) for a device, do the following: **NAS Management**→**NAS System**→ *Node (Server IP Address)*→**Devices**→ **Disks**.

## Displaying additional device-specific information

In order to display additional information for a device (for example, a fibre-channel adapter), use the NAS command **lscfg**.

### CLI command

At the command prompt, enter **lscfg**. This displays the devices in the system configuration.

Use the **-v** flag to display vital product data.

To display additional information for fibre-channel adapter 0, enter **lscfg -vl fcs0**.

For example, entering **lscfg -vl fcs0** would produce output similar to:

```
fcs0                U0.1-P2-I3/Q1  FC Adapter

Part Number.....00P4295
EC Level.....A
Serial Number.....1A3110034E
Manufacturer.....001A
FRU Number.....      00P4297
Network Address.....10000000C933161B
ROS Level and ID.....02E01035
Device Specific.(Z0).....2003806D
Device Specific.(Z1).....00000000
Device Specific.(Z2).....00000000
Device Specific.(Z3).....03000909
Device Specific.(Z4).....FF601032
Device Specific.(Z5).....02E01035
Device Specific.(Z6).....06631035
Device Specific.(Z7).....07631035
Device Specific.(Z8).....20000000C933161B
Device Specific.(Z9).....HS1.00X5
Device Specific.(ZA).....H1D1.00X5
Device Specific.(ZB).....H2D1.00X5
Device Specific.(YL).....U0.1-P2-I3/Q1
```

**Note:** The WWN (Network Address) and ROS Level and ID are shown here in bold for emphasis.

### SMIT fastpath

The SMIT fastpath is **smit lscfg**.

### WebSM

To view the Vital Product Data (VPD) for a device, do the following: **NAS Management**→**NAS System**→ *Node (Server IP Address)* →**Devices**→**Disks**→(right-click a disk)→**Vital Product Data**.

## Removing volume information from a local physical disk

If a volume has been exported from a system, you can format the disk that contains the volume so that the volume cannot be imported onto a system.

**Attention:** Data is lost with the use of this command.

### CLI command

At the command prompt, enter **chpvol -C hdiskname**.

### SMIT fastpath

The SMIT fastpath is **smit chpvol**.

### WebSM

In WebSM, do the following: **NAS Management**→**NAS System**→ *Node (Server IP Address)* →**Devices**→**Disks**→(right-click a disk)**Clear Volume Information**.

## Displaying the size of a remote disk

If a volume has been exported from a system, you can format the disk that contains the volume so that the volume cannot be imported onto a system.

**Attention:** Data is lost with the use of this command.



### CLI command

At the command prompt, enter **chpvol -C *hdiskname***.

### SMIT fastpath

The SMIT fastpath is **smit chpvol**.

### WebSM

In WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Disks**→(right-click a disk)→**Properties**.

## Removing volume information from a remote physical disk

If a volume has been exported from a system, you can format the disk that contains the volume so that the volume cannot be imported onto a system.

**Attention:** Data is lost with the use of this command.

### CLI command

At the command prompt, enter **chpvol -C *hdiskname***.

### SMIT fastpath

The SMIT fastpath is **smit chpvol**.

### WebSM

In WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Disks**→(right-click a disk).

## Creating a link aggregation device

You can create a link aggregation device.

### CLI command

At the command prompt, enter **mmlinkagg -e *adapterlist***.

### SMIT fastpath

The SMIT fastpath to create a link aggregation device is **smit mmlinkagg**.

### WebSM

To create a link aggregation device in WebSM, go to: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Communication**→**Overview and Tasks**→**Create a link aggregation**.

## Listing link aggregation devices

You can list configured link aggregation devices.

### CLI command

At the command prompt, enter **lslinkagg**.

### SMIT fastpath

The SMIT fastpath to list a link aggregation device is **smit lslinkagg**.

### WebSM

To list a link aggregation device in WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)** →**Devices**→**Communication**→**All Link Aggregations**.

## Changing a link aggregation device

You can change the configuration of a link aggregation.

### CLI command

At the command prompt, enter **chlinkagg -a aggregation**.

### SMIT fastpath

The SMIT fastpath to change a link aggregation device is **smit chlinkagg**.

### WebSM

To change a link aggregation device in WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)**→**Devices**→**Communication**→**Link Aggregations**→**(select a link aggregation device)**→**Change**.

## Removing a link aggregation device

You can remove a link aggregation device.

### CLI command

At the command prompt, enter **rmlinkagg -a aggregation**.

### SMIT fastpath

The SMIT fastpath to remove a link aggregation device is **smit rmlinkagg**.

### WebSM

To remove a link aggregation device in WebSM, do the following: **NAS Management**→**NAS System**→ **Node (Server IP Address)**→**Devices**→**Communication**→**Link Aggregations**→**(select a link aggregation device)**→**Delete**.

---

## Chapter 25. Managing file serving

The NAS Gateway 500 allows you to serve files using one or more protocols. The supported protocols are NFS, FTP, HTTP, and CIFS (for Windows users).

For each of these protocols, there are steps you need to take to configure the serving of files.

The section describes setup for the following protocols:

- FTP
- HTTP
- NFS
- CIFS

**Note:** CIFS is an optional feature of the NAS Gateway 500.

---

### FTP

The FTP file share protocol is enabled by default at system startup on the NAS Gateway 500.

#### Creating and managing FTP users

No configuration is necessary for users created on the NAS Gateway 500 for FTP access to their home directory. To create an FTP login, the NAS administrator can enter **smit ftp** at the command prompt. The Manage FTP panel displays two options:

- Create Anonymous FTP Login
- Create/Enable Anonymous FTP User Login

#### Creating an anonymous FTP login

To create an anonymous FTP login account, select **Create Anonymous FTP Login**. This account allows anonymous FTP access to files stored in the following directories:

- /home/ftp/bin
- /home/ftp/etc
- /home/ftp/pub
- /home/ftp/lib
- /home/ftp/dev
- /home/ftp/usr

This account owner can perform the following functions:

- Add user ftp
- Add user anonymous

The SMIT fastpath command is **mkanonftp**.

#### Creating or enabling an anonymous FTP login user

To create or enable an anonymous FTP user login account, select **Create / Enable Anonymous FTP User Login**. This allows the NAS administrator to create an anonymous FTP access for a file user's home directory. It also allows a subtree of

directories to be created. This option, when set to **yes**, creates the bin, pub, dev, etc, lib, and usr directories for this particular user.

The SMIT fastpath command is **mkanonftp**.

---

## HTTP

The NAS Gateway 500 has HTTP file sharing protocol preloaded on the system. It allows clients with a Web browser to access files stored on the NAS Gateway 500.

The NAS administrator can perform the following tasks:

- “Configuring the HTTP server”
- “Managing HTTP users” on page 127
- “Creating HTTP file shares” on page 128
- “Starting, restarting and stopping the HTTP serve daemon” on page 128
- “Starting, restarting, and stopping the HTTP administration server daemon” on page 129
- “Displaying HTTP server configuration information” on page 129
- “Displaying HTTP server logs” on page 130

You can use the SMIT fastpath **smit http** to perform HTTP-related administration functions.

### Configuring the HTTP server

This section describes the methods for configuring HTTP Server daemon for file share access. This operation is currently performed by the NAS administrator or root user, and is a command prompt configuration task. The HTTP file server takes its configuration in the form of server directives. The NAS Gateway 500 has a command prompt utility, **http\_config**, that controls the server directives. These directives are stored in two files:

- httpd.conf
- admin.conf

These files are located in the default directory `/usr/HTTPServer/conf`. The worksheet shown in Table 4 should be filled out before executing the **http\_config** application at the command prompt.

Table 4. HTTP configuration worksheet

Configuration description	Default value	User
Supply the group name to run HTTP Server	nasadm	
Supply the user ID to run HTTP Server	nasadmin	
Supply the HTTP server name	See Note <sup>1</sup>	
Supply the HTTP document root	/usr/HTTPServer/htdocs/	
Supply e-mail for the HTTP Server Administrator	User@ibm.com	
Allow for access control files to override Server Directives in httpd.conf	Yes	

<sup>1</sup> Host names are set during the initial configuration procedure. If this is not set, the default is the factory default which is the machine type model number and serial number. For example, IBM-5198001-10C2A9A

After completing the above worksheet, login in as root and execute **http\_config** from the /opt/nas/bin directory. At this point, the utility prompts you for the values on the HTTP Configuration worksheet.

The HTTP server configuration is complete. The following screen is displayed:

```

*****
-->
*****
Please supply the DocumentRoot of the HTTP Server
Default value --> /usr/HTTPServer/htdocs
*****
-->
*****
Please supply the email address for the admin
*****
-->youremail@yourcompany.com
*****
-->Please supply a filename to use for access control
Default value --> [.htaccess]
*****
-->
*****
Alloc access control files to override httpd.conf file?
Default valu --> [yes]
*****
-->
httpd restarted
Congratulations !!
HTTP configuration has been completed successfully !!
</opt/nas/bin>-->

```

## Managing HTTP users

This section describes how to manage the NAS Gateway 500 HTTP file shares. This section covers how to create the user password, how to create a share, how to limit access to shares created, and displays information about the HTTP file server. All these functions can be performed as NAS administrator or root user.

To create access for users on the HTTP file shares:

1. To allow access to file shares, a password must be generated for each file access user. This password is stored in a file, admin.passwd, in the directory /usr/HTTPServer/conf. Use the **htpasswd** command to create the password. The following is an example of an interactive session when using the **smit htpasswd** command:

```

                                Authenticate Users

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* User Name                                [Entry Fields]
Encryption                                [] +
Update File                                CRYPT +
                                           yes +

Esc+1=Help      Esc+2=Refresh      Esc+3=Cancel      Esc+4=List
Esc+5=Reset     Esc+6=Command    Esc+7=Edit        Esc+8=Image
Esc+9=Shell     Esc+0=Exit      Enter=Do

```

Supply the following information:

**User name**

The name of the file access user.

**Note:** The file access user should already exist.

**Encryption**

Encryption must be enabled for controlled access. Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for encryption options.

**Update file**

Specifying *yes* allows the *admin.passwd* file to be updated. This file contains the users and passwords.

**Note:** Passwords stored in *admin.passwd* are encrypted.

## Creating HTTP file shares

In the NAS Gateway 500 HTTP file server, the *Document Root* is the starting location for all HTTP file shares. This section describes how to create HTTP share access. This operation can be performed as NAS administrator or root user.

The default document root directory is */usr/HTTPServer/htdocs*. This is directory created during the execution of **http\_config**.

The **adhaccess** command performs the following operations:

- Provides permission to user or groups to an HTTP file share.
- Creates the *.htaccess* file.
- Allows the creation of NAS volumes as HTTP file share.
- Creates a symbolic link to NAS volumes or directories.

**Note:** Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for all options of this command.

The following panel can be accessed by entering **smit adhaccess**.

Configure HTTP Access

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

* User	[Entry Fields]
* Directory / File to Share	[fileusr1] + [/httpshares]+

Esc+1=Help	Esc+2=Refresh	Esc+3=Cancel	Esc+4=List
Esc+5=Reset	Esc+6=Command	Esc+7=Edit	Esc+8=Image
Esc+9=Shell	Esc+0=Exit	Enter=Do	

## Starting, restarting and stopping the HTTP serve daemon

The HTTP server daemon can be started, stopped and restarted by using the CLI or SMIT.

### **CLI command**

Use the command `apachectl`. This command can be invoked with the following arguments:

- **start**
- **stop**
- **restart**

### **SMIT fastpath**

The command can be accessed using the SMIT fastpath `smit http`.

Choose the appropriate action:

- **Start HTTP Service**
- **Restart HTTP Service**
- **Stop HTTP Service**

## **Starting, restarting, and stopping the HTTP administration server daemon**

The HTTP administration server daemon can be started, stopped and restarted by using the CLI or SMIT.

### **CLI command**

Use the command `adminctl`. This command can be invoked with the following arguments:

- **start**
- **stop**
- **restart**

This daemon turns on an additional administration port.

### **SMIT fastpath**

The command can be accessed using the SMIT fastpath `smit http`.

Choose the appropriate action:

- **Start HTTP Administration Service**
- **Restart HTTP Administration Service**
- **Stop HTTP Administration Service**

## **Displaying HTTP server configuration information**

The HTTP server contains two configuration files that have information about your HTTP server setup. Displaying this information can be used as a debug aid. These files are the `admin.conf` and `httpd.conf`.

### **CLI command**

To display information about your configuration, use the `lshttp` command. Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for information about all options for this command.

### **SMIT fastpath**

Use the SMIT fastpath `smit lshttp`.

The following information is displayed from this command:

```
COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

[TOP]
      /usr/HTTPServer/conf/admin.conf
DocumentRoot :
MaxClient    :
ServerName   :
ServerRoot   :/usr/HTTPServer
ServerPort   :8008
ServerType   :
User         :nobody
Group        :nobody
LogLevel     :
Timeout      :300
ErrorLog     :logs/admin_error.log
[MORE...19]
```

## Displaying HTTP server logs

The HTTP server contains logs that can be displayed and used to aid in configuration debug.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for information about all options for the **lshttplogs** command. This command is helpful when debugging problems with your HTTP server daemon.

### CLI command

Use the **lshttplogs** command.

### SMIT fastpath

The command can be accessed using the SMIT fastpath **smit lshttplogs**.

Select the appropriate logfile to display:

- access\_log
- error\_log
- httpd.pid

---

## Network File System

This section describes how to use Network File System (NFS). Subsections include:

- “Starting Network File System” on page 131
- “Stopping Network File System” on page 131
- “Changing Network File System characteristics” on page 131
- “Displaying currently exported volumes” on page 132
- “Adding a volume to the export list” on page 132
- “Exporting and recovering snapshot data” on page 133
- “Exporting all volumes” on page 134
- “Exporting a specific volume from the export list” on page 134
- “Changing or showing attributes of an exported directory” on page 134
- “Unexporting and removing a volume from the export list” on page 135
- “Unexporting all volumes” on page 135
- “Unexporting a specific volume” on page 135



- “Mounting a volume from an AIX client” on page 136
- “Displaying remotely mounted filesystems” on page 136
- “Starting PC NFS” on page 136
- “Stopping PC NFS” on page 137

## Starting Network File System

NFS is started during the NAS Gateway 500 boot process. Therefore, you only need to issue the **Start NFS** command if the **Stop NFS** command has been previously issued. In a clustered environment, issue the **Start NFS** command on the same node from which the **Stop NFS** command was issued.

NFS serves files as defined by the administrator (refer to the **mknasnfsexp**, **lsnasnfsexp**, **rmnasnfsexp**, or **chnasnfsexp** commands in the *IBM TotalStorage NAS Gateway 500 Command Reference*).

To start NFS:

1. SMIT menu fastpath: **smit nfs**
2. Select **Start NFS**.

Select one of the following options.

- |                |  |
|----------------|--|
| <b>both</b>    | This is the most common selection. It starts the NFS server immediately and every time the system reboots. |
| <b>now</b>     | Starts the NFS server immediately, but does not start the NFS server after reboot.                         |
| <b>restart</b> | Starts the NFS server only after the system has been rebooted.   |

## Stopping Network File System

To stop serving all NFS files:

1. Go to the SMIT menu fastpath: **smit nfs**
2. Select **Stop NFS**

Select one of the following options.

- |                |   |
|----------------|---|
| <b>both</b>    | This is the most common selection. It stops the NFS server immediately and does not start the NFS server after the system reboots.                          |
| <b>now</b>     | Stops the NFS server immediately. The system can be configured during setup to restart the NFS server automatically after the <b>now</b> command completes. |
| <b>restart</b> | Restarts the NFS server only after the system has been rebooted.  |

## Changing Network File System characteristics

You can change the number of NFS daemons that run on the system using the **chnfs** command.

### CLI command

Use the **chnfs** command.

In most situations the default values are appropriate. In configurations with very heavy NFS loads, performance gains may be seen by increasing the number of NFS daemons.

- n #** Specifies the number of nfsd (Server) daemons to run. At least one nfsd daemon must be run for NFS to work. The default value of 8 daemons can handle an average load. Heavy loads may require more daemons.
  - b #** Specifies the number of biod (Client) daemons to run. At least one biod daemon must be run for NFS to work. The default value of 6 daemons can handle an average load. Heavy loads may require more daemons.
  - l #** Specifies the maximum number of locked threads to run. The locked daemon handles requests to lock files, both from the local system and from remote clients. The default maximum of 33 can handle an average load. Heavy loads may require that the value be increased, up to a maximum of 511.
- N, -I, or -B**  
Specify that the change should apply now, at system restart, or both.

### SMIT fastpath

The SMIT fastpath to change NFS characteristics is:

1. Enter **smit nfs**.
2. Select **Change NFS Characteristics**.
3. Specify the numbers of NFS daemons that should run on the system.
4. Choose whether the change should apply now, at system restart, or both.

## Displaying currently exported volumes

To show the currently exported volumes:

1. Execute SMIT fastpath: **smit nfs**
2. Select **Display Currently Exported Volumes**.

In a single-node system, this command lists the volumes that are currently exported for NFS access. In a clustering (dual node) solution, you have the option of viewing only the volumes that are being exported by a particular node.

## Adding a volume to the export list

You can add a volume to the export list to make the volume available for NFS export so that client servers can mount the volume.

1. For this command, you can use the defaults in most situations. You must specify the directory to export. This directory almost always begins with `/Vols/`.
2. Enter the name of the volume to be exported after `/Vols/`. For example, `/Vols/VolumeName/`.
3. Enter the HOSTS & NETGROUPS that are allowed client access. You need to enter the client computers that are accessing the NFS export.
4. The Node/Group field is used only in a clustered environment. The Node/Group field must be used if you want to specify the Node/Group to which the export belongs.

If the system is clustered and no Node/Group is specified, the export is added to the Node/Group on which the command is being executed.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **mknasnfsexp** command.

## SMIT fastpath

The SMIT fastpath to add a volume to the export is:

1. Enter **smit nfs**.
2. Select **Add a Volume to Export List**.
3. Enter the full pathname of the directory to export.
4. Enter any hosts and netgroups allowed client access.
5. Modify any other parameters as needed for this particular export.

## Exporting and recovering snapshot data

The section describes how the NAS administrator can make a snapshot persistent for file user access. File users might need access to snapshots in order to restore copies of their own data from a certain snapshot without calling the NAS administrator or root user to roll back a file.

A snapshot can be directly exported and mounted using NFS.

### CLI command

1. Edit `/usr/sbin/cluster/etc/exports`. This file contains the NFS share permissions and configuration normally found in `/etc/exports`. A sample of this file is:  

```
/Vols/vol3
/Vols/vol3/.snapshot/snap1 -ro,access=192.168.3.223:192.168.3.194
- this is a sample line creating a read-only share of a snapshot for the specified hosts
```
2. At the command prompt, enter **exportfs -av -f /usr/sbin/cluster/etc/exports**.

**Note:** The command options are as follows:

- **-a** – export all mounts listed in exports file
- **-v** – verbose
- **-f** – use specified file in place of default `/etc/exports` file

**Note:** If you fail to edit `/usr/sbin/cluster/etc/exports` and specify this file when running **exportfs**, the NFS sharing of other volumes can be disrupted.

To view, read, and copy files from the snapshot, enter:

```
mkdir /snap1
mount 192.168.3.175:/Vols/vol3/.snapshot/snap1 /snap
```

**Note:** This solution is valid only on a single node configuration.

## SMIT fastpath

The SMIT menu fastpath command directly export and mount a snapshot file using NFS. is **smit nfs**.

1. Select **Add a Volume to Export List**
2. Specify the pathname of directory to export (full explicit pathname required) – for example, `/Vols/vol3/.snapshot/snap1`
3. Specify the mode to export directory by entering **ESC+4** and select **read-only HOSTS & NETGROUPS allowed client access**
4. Enter resolvable host names or IP address separated by spaces (for example, `192.168.3.223 192.168.3.194`). Subnets are valid.
5. Select **both** to indicate that the directory should be exported now and at system restart.

## Exporting all volumes

You can start exporting all the directories defined for export. Use the **exportnasfs** command when the directories are not exported at system startup.

In a clustered environment, the Node/Group field can be used to specify directories that only reside in one Node/Group

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **exportnasfs** command.

### SMIT fastpath

The SMIT fastpath to export all volumes is:

1. Enter **smit nfs**.
2. Select **Export All Volumes**.
3. Specify the Node/Group to begin exporting from by pressing **ESC+4** and select the Node/Group that should begin exporting all of its defined exports. If no Node/Group is specified, the default behavior is to export the directories from the local node.

## Exporting a specific volume from the export list

You can export a single directory from the list of exports. This command only exports one directory at a time.

In a clustered environment, the Node/Group field can be used to specify directories that only reside in one Node/Group.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **exportnasfs** command.

### SMIT fastpath

The SMIT fastpath to export a specific volume is:

1. Enter **smit nfs**.
2. Select **Export Specific Volume from Export List**.
3. Specify the directory to export by pressing **Esc+4**.

## Changing or showing attributes of an exported directory

You can modify all of the attributes specified after an export is defined. Use this command to add or remove clients that are allowed access to this export.

This command only applies to one share at a time.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **chnasnfsexp** command.

### SMIT fastpath

The SMIT fastpath to change or show attributes of an exported directory is:

1. Enter **smit nfs**.
2. Select **Change / Show Characteristics of Currently Exported Volume**.
3. Press **Esc+4** to select the export to change or show.
4. Modify any fields as needed.

## Unexporting and removing a volume from the export list

This command only applies to one exported directory at a time. This command stops all file access traffic and removes the directory from the list of those to be exported. The standard options of now, system restart, or both apply to this command.

- Now** Stops traffic immediately.
- Restart** Only affects the exports on system reboot.
- Both** Stops traffic now and traffic is not started again at system restart.

### CLI command

To use the command prompt to unexport or remove a volume from the export list, enter **rmnasfsexp**.

### SMIT fastpath

The SMIT fastpath to unexport or remove a volume from the export list is:

1. Enter **smit nfs**.
2. Select **Unexport and Remove Volume from Export List**.
3. Press **Esc+4** to select the directory to unexport and remove.

## Unexporting all volumes

This command stops all NFS traffic. No further NFS traffic is allowed.

In a clustered environment you can specify which Node/Group should stop exporting all volumes.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **exportnasfs** command.

### SMIT fastpath

The SMIT fastpath to unexport all volumes is:

1. Enter **smit nfs**.
2. Select **Unexport All Volumes**.
3. Optionally, select which Node/Group should stop its NFS access.

## Unexporting a specific volume

You can stop traffic to a specified directory.

### CLI command

Use the **exportnasfs** command to stop NFS traffic to the specified directory. No NFS traffic is allowed to that directory.

This command applies to only one export at a time.

Refer to the *IBM TotalStorage NAS Gateway 500 Command Reference* for the syntax and parameter description for the **exportnasfs** command.

### SMIT fastpath

The SMIT fastpath to unexport a specific volume is:

1. Enter **smit nfs**.
2. Press **Esc+4** to select the directory to be unexported.

## Mounting a volume from an AIX client

In a clustered environment, you can specify the host name of a node in the **mount** command, because during a failover, the operating node assumes the host name (alias) of the failed node.

For example:

**mount GatewayNode1:/Vols/Vol1/Pensions/NAS**

- GatewayNode1 is the hostname
- Vols is the standard root prefix
- Vol1 is the Volume name
- Pensions is the directory
- /NAS = mount point of the AIX client

## Displaying remotely mounted filesystems

You can display all filesystems that are currently mounted from a remote client.

### CLI command

To display all filesystems that are currently mounted from a remote client, use the **showmount** command.

- a** Displays the remote mounts in the format hostname:filesystem.
- d** Displays only the names of the filesystems that are currently mounted remotely.

### SMIT fastpath

The SMIT menu fastpath to display remotely mounted filesystems is:

1. Enter **smit nfs**.
2. Select **Display remotely mounted filesystems**.
3. Select **Show All Clients and Directories Mounted by Clients** to show all remote mounts in the format hostname:filesystem or select **Show Only Which Directories are Mounted** to see a list of the filesystems that are currently mounted remotely.

## Starting PC NFS

You can start the `rpc.pcnfsd` daemon, which handles requests from PC-NFS clients for authentication services on remote machines. These services include authentication for mounting and for print spooling. The PC-NFS program allows personal computers running DOS to be networked with machines running NFS. It is usually not necessary to change the default values of the options.

### CLI command

To start PC NFS services using the command line, use the **mkpcnfs** command.

- p** Specifies the Internet transfer protocol the `rpc.pcnfsd` daemon should listen for requests on. Valid values are `udp`, `tcp`, `udp6`, and `tcp6`.
- t** Specifies the type of socket the `rpc.pcnfsd` daemon should use. Valid values are `stream` and `dgram`.
- w** Determines whether the `inetd` daemon waits for a datagram server to release the socket before continuing to listen at the socket. Valid values are `wait`, `nowait`, or `SRC`. The `SRC` value works like `wait`, but instead of forking and waiting for the child to die, it does a `startsrc` on the subsystem and

stores information about the starting of the service. When the service is removed, it then has a stopsrc issued to the service to stop it.

### SMIT fastpath

The SMIT fastpath to start PC NFS services is:

1. Enter **smit nfs**.
2. Select **Start PC NFS**.
3. If desired, modify default values for the protocol, socket type, and wait indicator (if multiple protocols are desired, each must be started separately).

## Stopping PC NFS

You can stop the rpc.pcnfsd daemon.

### CLI command

To stop PC NFS services using the command line, use the **rmpcnfs** command.

### SMIT fastpath

The SMIT fastpath to stop PC NFS services is:

1. Enter **smit nfs**.
2. Select **Stop PC NFS**.
3. Specify the protocol to stop. If multiple protocols have been started, each must be stopped separately.

---

## Common Internet File System

This section describes how to use the Common Internet File System (CIFS). For more information on configuring and administering the CIFS server, refer to the *IBM TotalStorage NAS Gateway 500 CIFS File Serving Guide*.

**Note:** CIFS file serving is an optional feature of the NAS Gateway 500. This feature must be enabled to use the commands in this chapter.

The NAS Gateway 500 contains Common Internet File System (CIFS) server software to provide file sharing to Windows clients.

CIFS server tasks are:

- “Starting the CIFS server” on page 139
- “Stopping the CIFS server” on page 139
- “CIFS server status” on page 139
- “CIFS server statistics” on page 139

CIFS configuration tasks are:

- “CIFS basic setup” on page 140
- “CIFS authentication” on page 141
- “CIFS resource limits” on page 142
- “CIFS fileserver characteristics” on page 142

CIFS file share tasks are:

- “Listing all currently available CIFS Shares” on page 143
- “Creating a CIFS share” on page 143
- “Changing attributes of a CIFS share” on page 144

- “Removing a CIFS share” on page 144

CIFS user tasks are:

- “Listing all CIFS users” on page 144
- “Mapping a Windows user to a NAS file access user” on page 145
- “Creating a CIFS user” on page 145
- “Changing a CIFS user” on page 146
- “Changing a CIFS user’s password” on page 146
- “Removing a CIFS user” on page 146

Before administering the CIFS server, read “CIFS concepts.”

## CIFS concepts

There are two parts to granting a Windows user access to a CIFS Share.

1. Map the user to a NAS file access user. This allows the NAS Gateway 500 to handle file permissions and access rights. See “User mapping.”
2. Authenticate the user to prove that the user is allowed access. See “Authentication”

### User mapping

All Windows users accessing CIFS Shares on the NAS Gateway 500 must be mapped to a NAS file access user. If the Windows and NAS file access user names are identical, the user is mapped automatically. When the user names do not match, a NAS administrator must define a user mapping so that the NAS Gateway 500 can authenticate and handle the Windows user. See “Mapping a Windows user to a NAS file access user” on page 145 for instructions to create these mappings.

### Authentication

To access shares on the CIFS server, a Windows user must be authenticated. The CIFS server can handle authentication in two ways, passthrough and local. The authentication method is selected during initial configuration in the CIFS Wizard.

Passthrough authentication is commonly used in Microsoft Active Directory or Windows NT Domain environments. The authentication request is passed to an Active Directory Server (ADS) or Primary/Backup Domain Controller (PDC/BDC), which checks the password. This is the preferred method of operation for the NAS Gateway 500.

Local authentication is used if an ADS or PDC/BDC is not available. All password authentication is handled by the NAS Gateway 500. Passwords can be encrypted or plain text.

Plain text passwords are insecure, but require little administrative overhead. CIFS requests are authenticated against the standard system user registry. The password is compared against the associated NAS file access user’s password.

Encrypted passwords are more secure, but require the NAS administrator to define a CIFS user for each NAS file access user account that is used to access CIFS files. The CIFS user essentially stores an encrypted CIFS password for a NAS file access user. See “Creating a CIFS user” on page 145 for instructions to create the CIFS user.



## Starting the CIFS server

If the CIFS server is not running, it can be started by a NAS administrator. When the CIFS file serving feature is enabled, the CIFS server is started automatically by the NAS Gateway 500. However, you may need to restart the CIFS server for configuration changes to take effect or after service.

**Note:** In a clustered environment, the commands in this section start the CIFS server on the node that you are currently managing. In order to start the CIFS server on any other node, you must log in to that node and issue the command again.

To start the CIFS server:

### CLI command

At the command prompt, enter **net start**.

### SMIT fastpath

The SMIT menu fastpath command to start a CIFS server is **smit cifs**. Then select **Start CIFS Server**.

## Stopping the CIFS server

You might need to stop the CIFS server while the NAS Gateway 500 is still running. Generally, this is when the CIFS server settings have changed and the CIFS server needs to be restarted or during service.

**Note:** In a clustered environment, the commands in this section stop the CIFS server on the node that you are currently managing. In order to stop the CIFS server on any other node, you must log in to that node and issue the command again.

To stop the CIFS server:

### CLI command

At the command prompt, enter **net stop**.

### SMIT fastpath

The SMIT menu fastpath command to stop a CIFS server is **smit cifs**. Then select **Stop CIFS Server**.

## CIFS server status

You can query the operational status of the server.

### CLI command

At the command prompt, enter **net status**.

### SMIT fastpath

The SMIT menu fastpath command to stop a CIFS server is **smit cifs**. Then select **Server Status**.

## CIFS server statistics

You can list the statistics on server resources since it was started or reset.

### CLI command

At the command prompt, enter **net statistics**.

## SMIT fastpath

The SMIT menu fastpath command to stop a CIFS server is **smit cifs**. Then select **Server Statistics**.

## CIFS basic setup

Basic setup sets the CIFS parameters for your configuration.

### CLI command

#### Server Name

The name of the server. The name of the CIFS server defaults to the TCP/IP hostname of the machine. Use this field to change the server name. A CIFS server name can be no longer than 15 characters.

#### Start Server

Starts the CIFS server. This enables clients to access all of the resources (shares) that the server has defined.

#### Domain Name

Specify the name of the domain to which this server belongs. The Domain Name is the name assigned to a group of servers that interoperate to provide resources as a single unit.

#### Description

Description comments for this server.

#### Server alias(es)

Displays server alias(es)

#### WINS Address

Specify the full IP address of the machine that acts as the Windows Internet Name Service (WINS) server. The WINS server provides a NetBIOS name service in which the server keeps a table of names on the subnetwork and their IP addresses. The internet address uses dotted decimal form, such as d.d.d.d, where "d" is a decimal value from 0 to 255, inclusive.

#### Backup WINS address

The Backup WINS Address is the IP address of the WINS server that is used when the primary WINS server is not available. Specify the internet address in the following format: d.d.d.d, where "d" is a decimal value from 0 to 244, inclusive. This field is optional.

#### Proxy WINS Server

The WINS proxy server allows clients without WINS capability to work with a WINS server. The WINS proxy server interoperates with non-WINS clients using Broadcast Node protocol and communicates with the WINS server on their behalf. This field is optional.

#### NetBIOS Name Server (NBNS)

Allows you to add, delete, back up, restore, and list the NetBIOS Names entries that the WINS server keeps in its table. A NetBIOS Name Server can be no longer than 15 characters.

#### NetBIOS Datagram Server

If enabled, AIX Fast Connect server supports NetBIOS DataGram service

#### Master Browser

Specifies if CIFS can act as a Master Browser for its domain/workgroup.

#### Multi-Session support

Specifies if multiple user sessions from a single workstation is supported. Do not use this with the network logon feature.

## SMIT fastpath

The SMIT menu fastpath command to set up CIFS is **smit cifs**. Then select **CIFS Configuration** and then select **Basic Setup**.

## CIFS authentication

To perform CIFS authentication, use the SMIT fastpath **smit cifs**.

### SMIT fastpath

The SMIT menu fastpath command to perform CIFS authentication is **smit cifs**.

1. Select **CIFS Configuration and Authentication**.
2. Then select one of the following:

#### Authentication (General)

Sets the following general CIFS parameters:

##### Use Encrypted Passwords

Prevents client passwords from being accepted in encrypted form in the session set up with the server.

##### Client user name mapping

Specifies if the User Name Mapping feature is enabled.

##### Enable Guest-mode logon

Specifies whether or not guest access is allowed.

##### Guest logon ID

Specifies the logon name to be used as guest on the server.

##### Enable share level security

Specifies if share level security should be enabled instead of user level security.

##### Share level security user login

Specifies the user name to be used for file access credentials when share level security is enabled.

#### Remote Authentication options

Sets the following CIFS parameters:

##### CIFS Passthrough authentication server

Specifies the IP address of the passthrough authentication server.

##### CIFS Backup authentication server

Specifies the IP address of the backup passthrough authentication server.

##### Kerberos-based authentication

Specifies whether Kerberos based authentication should be used. If you enable Kerberos based authentication, then you must also specify the Kerberos service name. The Kerberos service name specifies the service name of the Kerberos domain controller to which the CIFS server authenticates Kerberos users when the Kerberos based authentication feature is enabled.

##### LDAP settings

Defines the following LDAP settings:

- LDAP-based authentication
- LDAP server name

- LDAP user context (DN)
- LDAP administrator account
- Keytab file for LDAP access

### **Network Logon**

Sets the following parameters:

- Enable network logon server for client PCs
- Profiles path type
- Profiles path
- Network logon path
- Client startup script file name
- Allow clients to remotely change passwords
- Synchronize changed passwords with system

## **CIFS resource limits**

You can set the following parameters:

- Maximum users
- Maximum connections
- Maximum open
- Maximum searches
- Auto disconnects
- Maximum number of shares

### **SMIT fastpath**

The SMIT menu fastpath command to perform CIFS authentication is **smit cifs**.

1. Select **CIFS Configuration**.
2. Select **Resource Limits**.

## **CIFS fileserver characteristics**

You can set the following parameters:

- Enable opportunistic locking
- Enable search caching
- Enable send file API support
- Umask
- Preserve mixed-case filenames
- JFS ACL-inheritance
- DOS File Attributes support
- Map long filenames to DOS 8.3 filenames
- DOS filename-mapping character
- Enable memory-mapped files
- Unicode conversions (double byte characters)
- Enable MSDFS support
- MSDFS load-leveiling

### **SMIT fastpath**

The SMIT menu fastpath command to perform CIFS authentication is **smit cifs**.

1. Select **CIFS Configuration**.
2. Select **Fileserver characteristics**.

## Listing all currently available CIFS Shares

A NAS administrator can list the currently defined CIFS Shares. In a clustered environment, only shares that are currently available on the current node are listed.

### SMIT fastpath

The SMIT menu fastpath command to list the currently defined CIFS Shares is **smit cifs**.

1. Select **File shares**
2. Select **List all CIFS Shares**

SMIT displays a list of the current CIFS Shares with names, paths, and descriptions.

## Creating a CIFS share

To allow Windows users to access files on the NAS Gateway 500, a NAS administrator must define CIFS shares.

**Note:** When Remote Mirroring is enabled, you must disable the cluster to perform this operation. Then create the CIFS share, re-enable the cluster, and wait for the cluster to resynchronize.

To create a CIFS share:

### SMIT fastpath

The SMIT menu fastpath command to define CIFS Shares is **smit cifs**.

1. Select **File Shares**.
2. Select **Add a CIFS Share**.
3. Fill in the required fields.

The commonly used fields in the dialog are:

<b>Share (network) Name</b>	The name of the CIFS share. The share name does not have to be the same as the directory, but it must be unique across all CIFS shares on the NAS Gateway 500. Clients access the share with the Universal Naming Convention (UNC) path \\servername\sharename (where <i>servername</i> is the NetBIOS name of the server hosting the share and sharename is the share name you specify).
<b>Path</b>	Specifies the NAS Gateway 500 filesystem path to share. This path must already exist and it must reside on a NAS volume. For example, if you have a volume called HRVol with a subdirectory Pensions you want to share, the path would be /Vols/HRVol/Pensions (all NAS volumes are mounted under the directory /Vols).
<b>Description</b>	Text comment that appears next to the share name in the CIFS server's share list and in the Windows network browser.

The remaining fields can be left at the default settings. Refer to the *IBM TotalStorage NAS Gateway 500 CIFS File Serving Guide* for details.

The share is available immediately in a single-node NAS Gateway 500. In a clustered environment, the share is available after the cluster has resynchronized. During cluster synchronization, the NAS Gateway 500 might become temporarily unavailable.

## Changing attributes of a CIFS share

A NAS administrator can modify the current attributes of a CIFS share.

In a clustered environment, this command operates only on the node that you are currently managing (logged in on). In order to perform this operation on any other node, you must log in to that node and issue the command again.

**Note:** When Remote Mirroring is enabled, you must disable the cluster to perform this operation. Then change the CIFS share, re-enable the cluster, and wait for the cluster to resynchronize.

### SMIT fastpath

The SMIT menu fastpath command to change attributes of a CIFS share is **smit cifs**.

1. Select **File Shares**.
2. Select **Change a CIFS Share**.
3. Select the CIFS share you want to change.
4. Change any fields necessary.

The changes take effect immediately in a single-node NAS Gateway 500. In a clustered environment, the changes take effect after the cluster has resynchronized. During cluster synchronization, the NAS Gateway 500 might become temporarily unavailable.

## Removing a CIFS share

When a CIFS share is no longer needed, a NAS administrator can delete it.

In a clustered environment, this command operates only on the node that you are currently managing (logged in on). In order to perform this operation on any other node, you must log in to that node and issue the command again.

**Note:** When Remote Mirroring is enabled, you must disable the cluster to perform this operation. Then delete the CIFS share, re-enable the cluster, and wait for the cluster to resynchronize.

### SMIT fastpath

The SMIT menu fastpath command to remove a CIFS Share is **smit cifs**.

1. Select **File Shares**.
2. Select **Remove a CIFS Share**.
3. Select the CIFS Share you want to delete.
4. Change any fields necessary.

The deletion takes effect immediately in a single-node NAS Gateway 500. In a clustered environment, the deletion takes effect after the cluster has resynchronized. During cluster synchronization, the NAS Gateway 500 might become temporarily unavailable.

## Listing all CIFS users

A NAS administrator can view a list of the current CIFS users.

### CLI command

At the command prompt, enter **net user**.

### SMIT fastpath

The SMIT menu fastpath command to view a list of the current CIFS users and mappings is **smit cifs**. Then

1. Select **CIFS Users**.
2. Select **List all CIFS Users**.

SMIT displays a list of the current CIFS users by Windows name, NAS file access user name and description.

## Mapping a Windows user to a NAS file access user

When the Windows name of a CIFS user is not the same as their NAS file access user name, a NAS administrator can create a user name mapping.

### SMIT fastpath

The SMIT menu fastpath command to map a Windows user to a NAS file access user is **smit cifs**. Then

1. Select **CIFS Users**.
2. Select **Map a CIFS User**.
3. Fill in the required fields.

The fields in the dialog are:

<b>Client user name</b>	Specifies the Windows user name.
<b>Server user name</b>	Specifies the NAS file access user to which you would like to map the Windows user. Press <b>Esc+4</b> or <b>F4</b> to bring up a list of users.
<b>Description</b>	Optional text field describing the mapping.
<b>Active</b>	Indicates whether this user is able to connect to the CIFS server. Generally, this should be left as <i>yes</i> .

You can map multiple Windows users to the same NAS file access user. If you are not using passthrough authentication, all Windows users mapped to the same NAS file access user must have the same password.

## Creating a CIFS user

When the NAS Gateway 500 is configured to perform encrypted CIFS authentication locally, each NAS file access user account that is used for CIFS access must have a CIFS password defined. To define this password, a NAS administrator should create a CIFS user.

### SMIT fastpath

The SMIT menu fastpath command to create a CIFS user is **smit cifs**. Then

1. Select **CIFS Users**.
2. Select **Add a CIFS User**.
3. Fill in the required fields.
4. At the prompt, enter the CIFS password for the user.

The fields in the dialog are:

<b>User name</b>	Specifies the NAS file access user for whom you are defining the password. Press <b>Esc+4</b> or <b>F4</b> to bring up a list of users.
<b>Description</b>	Optional text field describing the user.
<b>Active</b>	Indicates whether this user is able to connect to the CIFS server. Generally, this should be left as <i>yes</i> .
<b>Hide/show password</b>	Determines whether the password prompt echoes the password.

The CIFS password should be identical to the user's Windows password.

## Changing a CIFS user

An existing CIFS user or mapping can be modified by a NAS administrator. To change their password, see "Changing a CIFS user's password."

### SMIT fastpath

The SMIT menu fastpath command to start a CIFS server is **smit cifs**.

1. Select **File CIFS Users**.
2. Select **Change a CIFS User**.
3. Select the CIFS user you want to change.
4. Change any fields necessary.

The field **Server user name** is only applicable to user mappings.

## Changing a CIFS user's password

A NAS administrator can change a CIFS user's password.

To change a CIFS user's password:

### CLI command

At the command prompt, enter **net user *username* -p**.

### SMIT fastpath

The SMIT menu fastpath command to change a CIFS user's password is **smit file\_user\_local**. Then

1. Select **CIFS Users**.
2. Select **Set / Change a CIFS User's Password**.
3. Select a CIFS user.
4. Enter the password at the prompt.

The CIFS user selection displays all CIFS users and mappings. If you select a user mapping rather than a CIFS user, you receive an error following the password prompt.

## Removing a CIFS user

When a CIFS user or mapping is no longer needed, a NAS administrator can delete it.

To remove a CIFS user:

### CLI command

At the command prompt, enter **net user /delete *username***.



## SMIT fastpath

The SMIT menu fastpath command to remove a CIFS user is **smit cifs**. Then

1. Select **CIFS Users**.
2. Select **Remove a CIFS User**.
3. Select the CIFS user or mapping you want to delete.

The SMIT menu lists the CIFS users by their Windows username.

---

## NetBIOS Name Server

You can add, delete, back up, restore, and list the NetBIOS names and types of names that the NetBIOS server keeps in its table. Names added to the table are considered static names and do not need to be refreshed. Client machines cannot delete these names.

NetBIOS Name Server (NBNS) tasks are:

- “Listing names in the NetBIOS Name Table”
- “Adding a NetBIOS name”
- “Deleting a NetBIOS name”
- “Deleting a NetBIOS name by address and by name”
- “Backing up a NetBIOS Name table” on page 148
- “Restoring a NetBIOS Name table” on page 148

### Listing names in the NetBIOS Name Table

Lists the NetBIOS Names entries that the WINS server keeps in its table. Configuring the names is optional. Names added to the table are considered static names and are not required to be refreshed. Client machines cannot delete the names. They must be deleted by using the SMIT **delete name** option.

To list names in the NetBIOS Name Table:

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **List Names in NetBIOS Name Table**.

### Adding a NetBIOS name

You can add a NetBIOS name to the WINS name table.

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **Add a NetBIOS Name**.

### Deleting a NetBIOS name

You can delete a NetBIOS name from the WINS name table.

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **Delete a NetBIOS Name**.

### Deleting a NetBIOS name by address and by name

You can delete a NetBIOS name from the WINS name table and delete its IP address.

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **Delete by Address and by Name**.

## Backing up a NetBIOS Name table

You can back up the information in the name table to a file. The default file is `/etc/cifs/nbns.names`. This file is in a form that can be used to restore names. If you want to change the default file name, specify a fully qualified file name with the path.

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **Back up NetBIOS Name Table to a File**.

## Restoring a NetBIOS Name table

You can restore the information in the name table to a previous state using the `/etc/cifs/nbns.names` default backup file or another backup file. You must specify the backup file name as a fully qualified file name with the path.

1. Use the **smit cifs** command.
2. Select **NBNS**.
3. Select **Restore a NetBIOS Name Table from Back up File**.

---

## Chapter 26. Managing networking

The IBM TotalStorage NAS Gateway 500 supports up to four Ethernet adapters, allowing connectivity for up to eight physical Ethernet ports. That is, you can connect up to eight physical ports using four dual-port Ethernet adapters.

Because the NAS Gateway 500 supports PCI-X adapters, you do not need to shut down the system and remove the power cables before adding or replacing an adapter. For additional information about installing and removing adapters refer to the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*.

**Note:** Adding or removing hardware can require root authority.

This section discusses the basic configuration of network adapters and interfaces. For advanced configuration, refer to the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.

When a new network adapter is physically installed in the system, the operating system automatically adds the appropriate network interface for that adapter. For example, if you install an Ethernet adapter in your system, the operating system assigns it the name *ent0* and adds both an Ethernet Version 2 and an IEEE 802.3 interface, named *en0* and *et0*, respectively. In most cases, there is a one-to-one correspondence between adapter names and network interface names. For example, Ethernet adapter *ent0* corresponds to interface *en0* (for Ethernet Version 2) and *et0* (for IEEE 802.3).

At each system startup, the operating system automatically configures the network interface software based upon the information in the ODM database. Initially, the network interface is configured with default values. In order to communicate through a given network interface, you must set the Internet Protocol (IP) address. All other necessary attributes can use the default values. Provided below are several networking tasks and methods used to execute these tasks using CLI, SMIT and WebSM.

---

### Tasks used to manage networking

The following sections describe how to perform several networking tasks:

- “Listing Network Adapters and Interfaces”
- “Configuring network adapters using TCP/IP” on page 150
- “Obtaining network interface statistics” on page 150

### Listing Network Adapters and Interfaces

You can list network adapters and the network interfaces that are installed within the NAS Gateway 500 using one of the following methods:

#### CLI command

The root user can enter `lsparent -C -k ent` at the command prompt to display a list of the Ethernet devices within the device configuration database. You must have root user authority to perform this operation.

The root user can enter `lsdev -l en*` at the command prompt to list available Ethernet devices and interfaces in the system and their characteristics. You must have root user authority to perform this operation.

### SMIT fastpath

A list of all network interfaces can be accessed through the SMIT fast path by executing **smit lsinet**.

### WebSM

As a NAS administrator, you can display network interfaces and their status by executing the following from WebSM: **NAS Management** → **NAS System** → **xx.xx.xx.xx** (select your system) → **Network** → **TCP/IP (IPv4 and IPv6)** → **Network Interfaces**.

As a root user, you can access Communication Devices and their properties by executing the following path within WebSM: **Management Environment** → **xx.xx.xx.xx** (select your system) → **Devices** → **Communications**.

## Configuring network adapters using TCP/IP

You can configure the network adapter and the network interfaces that are detected on the NAS Gateway 500 using one of the following methods:

### CLI command

At the command prompt, enter **ifconfig**. This command allows you to assign an address to a network interface and has the capability to configure or display the current network interface configuration information.

**Attention:** Using the **ifconfig** CLI command to make updates does not save the configuration information into the ODM, and the changes are lost after a reboot. Both SMIT and WebSM update the ODM, so that configuration changes are persistent after a reboot.

### SMIT fastpath

As a NAS administrator, you can display or change the standard network TCP/IP interface characteristics using the SMIT fastpath to **NAS System Management** → **Manage Network** → **Configure TCP/IP** → **Minimum Configuration and Startup**. Then select the appropriate adapter.

The SMIT fastpath command **smit tcpip** provides direct access to the TCP/IP menu and the fastpath **smit chinet** provides direct access to the basic characteristics of the network interfaces.

### WebSM

As a NAS administrator, you can show or change network TCP/IP interfaces characteristics from the main WebSM panel by selecting **NAS Management** → **NAS System** → **xx.xx.xx.xx** (select your system) → **Network** → **TCP/IP (IPv4 and IPv6)** → **Network Interfaces**. Then right-click and select **Properties**.

## Obtaining network interface statistics

Use one of the following methods to display the statistical data for various network-related data structures for active connections:

### CLI command

At the command prompt, enter **netstat**. The **netstat** command symbolically displays the contents of various network-related data structures for active connections. For additional information, refer to the **netstat** command in the *IBM TotalStorage NAS Gateway 500 Command Reference*, or execute **man netstat** from the system prompt to display help.

### SMIT fastpath

As a NAS administrator, you can obtain network interface statistics by selecting **Manage System**→**System Information**→**Show Network Statistics**.

### WebSM

As a NAS administrator, you can obtain network interface statistics by executing **NAS Management**→**NAS System**→ **xx.xx.xx.xx** (IP address)→**Network**→**TCP/IP (IPv4 and IPv6)**→**Network Interfaces**→(right-click an interface)→**Network Statistics**.

## Configuring static routes

You can configure static routes for each of the interface that are detected on the NAS Gateway 500 using one of the following methods:

### CLI command

At the command prompt, enter `mkroute -d destination -g gateway`.

### SMIT fastpath

The SMIT fastpath command to make an static route is **smit mkroute**.

### WebSM

In WebSM, you can access the static routing wizard by navigating to: **NAS Management**→**NAS System**→**Node (Server IP address)**→**Network**→**Overview and Tasks**→**Static Route Wizard**.

## Removing static routes

You can remove a static route from a local node or its peer node.

### CLI command

At the command prompt, enter `rmroute -d destination -g gateway`.

### SMIT fastpath

The SMIT fastpath command to remove a static route is **smit rmroute**.

### WebSM

In WebSM, you can access the static routing wizard by navigating to: **NAS Management**→**NAS System**→**Node (Server IP address)**→**Network**→**Overview and Tasks**→**Static Route Wizard**.

## Listing static routes

You can list the static routes that are on a local node or its peer node.

### CLI command

At the command prompt, enter `lsroute`.

### SMIT fastpath

The SMIT fastpath command to remove a static route is **smit lsroute**.

### WebSM

In WebSM, you can access the static routing wizard by navigating to: **NAS Management**→**NAS System**→**Node (Server IP address)**→**Network**→**Overview and Tasks**→**Static Route Wizard**.



---

## Chapter 27. Managing security

In addition to the standard UNIX authentication system, the NAS Gateway 500 support for NFS includes an authentication system that can be used by other UNIX and non-UNIX systems. The system uses Data Encryption Standard (DES) encryption and public key cryptography to authenticate both users and machines in the network.

NFS uses the DES algorithm for different purposes. NFS uses DES to encrypt a time stamp in the Remote Procedure Call (RPC) messages sent between NFS servers and clients. This encrypted time stamp authenticates machines just as the token authenticates the sender.

Because NFS can authenticate every RPC message exchanged between NFS clients and servers, this provides an additional, optional level of security for each file system. By default, file systems are exported with the standard UNIX authentication. To take advantage of this additional level of security, specify the secure option when you export a file system.

---

### Tasks used to manage NFS and NIS security

The **smit nfs\_security** menu displays all of the options that can be selected for secure network service management. Use the following tasks to manage security:

- “Starting the keyser daemon”
- “Stopping the keyser daemon” on page 154
- “Adding or changing a user’s key” on page 154
- “Decrypting and storing a secret key” on page 154
- “Deleting a stored secret key” on page 154
- “Changing encryption key” on page 155

### Starting the keyser daemon

The keyser daemon stores the private encryption keys of each user logged into the system. When a user enters a password during a keylogin, the secret key is decrypted. The decrypted key is then stored by the keyser daemon. These decrypted keys enable the user to access secure network services such as secure Network File System (NFS). The secure network services, keyser daemon, can be enabled and disabled by using the CLI, SMIT or WebSM interface.

#### CLI command

To start the keyser daemon, the service can be enabled by using the System Resource Controller command, **startsrc -s keyser**.

To start the keyser daemon from the command line, execute the **mkkeyser** command

#### SMIT fastpath

This action can be performed using the SMIT fastpath **smit mkkeyser**.

#### WebSM

To enable secure network services using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems**, select **Configure Secure NFS**, and select **Start Key Service**.

## Stopping the keysevr daemon

The keysevr daemon can be disabled in the following ways:

### CLI command

To disable the keysevr daemon from the command prompt, execute the **rmkeysevr** command.

### SMIT fastpath

Use the SMIT fastpath **smit rmkeysevr**.

### WebSM

To disable secure network services using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems** and select **Unconfigure Secure NFS**.

## Adding or changing a user's key

Adding or changing a public key for a user can be done using the following methods:

**Note:** These keys are needed for using secure Remote Procedure Call (RPC) protocol or secure network.

### CLI command

At the command prompt, enter **newkey**.

### SMIT fastpath

Use the SMIT fastpath **smit newkey**.

### WebSM

To add or change a user's public key using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems**, select **Configure Secure NFS** and then select **User Keys**.

## Decrypting and storing a secret key

Decrypting and storing a public key for a user can be done using the following methods:

### CLI command

Execute the command from designated path: **keylogin**

### SMIT fastpath

Use the SMIT fastpath **smit keylogin**.

### WebSM

To decrypt and store a key using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems**, select **Configure Secure NFS** and select **User Keys**.

## Deleting a stored secret key

Deleting a stored secret key for a user can be done using the following methods:

**Note:** These keys are needed for using secure Remote Procedure Call (RPC) protocol or secure network.



### **CLI command**

At the command prompt, enter **keylogout**

### **SMIT fastpath**

Use the SMIT fastpath **smit keylogout**.

### **WebSM**

To delete a stored key using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems**, select **Configure Secure NFS** and select **User Keys**.

## **Changing encryption key**

Changing a public key for a user can be done using the following methods:

### **CLI command**

At the command prompt, enter **chkey**.

### **SMIT fastpath**

Use the SMIT fastpath **smit chkey**.

### **WebSM**

To change the encryption key using WebSM, execute the following: **NAS Management**→**NAS System**→**File Serving**→**Network File System**. From the Menu Bar, right-click **Network File Systems**, select **Configure Secure NFS** and select **User Keys**.



---

## Chapter 28. Managing the system

There are a number of system-related tasks that you can perform on the NAS Gateway 500. These include:

- Backup and Recovery of the system itself and associated configuration files
- Boot and Shutdown options
- Date and Time settings
- Problem Determination
- System Information

---

### Backup and recovery of the system

This section describes several options available to the NAS administrator or root user for creating backups using tape and disk devices.

Backup and Recovery using Tivoli Storage Manager (TSM) is described in “Using Tivoli Storage Manager (TSM)” on page 93. The SMIT path **SMIT→Manage System→Backup and Recovery→Backup and Recovery with Tivoli Storage Manager (TSM)** results in the same menus as **SMIT→Managing Applications**.

The NAS administrator can backup the NAS system software using the **smit backup** command or **SMIT→Manage System→Backup and Recovery→Backup System to Tape / File**.

The command **listvgbackup** displays a list of files in a system backup. This function is also available using **SMIT→Manage System→Backup and Recovery→List Files in System Backup**.

### Backup configuration files

After you perform the initial configuration and after making subsequent configuration changes on the NAS Gateway 500, you might want to perform a backup of the configuration files where your unique configuration information is stored. This information is valuable in the event that you need to restore your system.

You can backup these configuration files using the SMIT fastpath **smit mknasb**.

### Restore configuration files

If you need to restore your system or need to restore the set of configuration files that contain your unique configuration information, you can do so using a backup that you have previously created.

**Attention:** Restoring the configuration files overwrites any existing configuration files. You should maintain a backup of your existing configuration files before you attempt to restore a previous configuration.

You can restore configuration files using the SMIT fastpath **smit restnasb**.

---

### Boot and shutdown

The following sections describe booting and shutdown:

- “Shutdown the system” on page 158
- “Changing reboot options” on page 158

## Shutdown the system

The **shutdown** command halts the NAS Gateway 500 system software. Any root user login sessions or NAS administrator login sessions are sent a message of the impending system shutdown.

**Note:** Do not attempt to restart the system or turn off the system before the shutdown completion message is displayed; otherwise file system damage can result.

You can initiate the shutdown of the system using the SMIT fastpath **smit shutdown**.

If you have systems clustered together and are planning to shut down one node, and want to have files currently being served by the node being shut down to be served by the other node in the cluster, then you need to relocate the volumes from the node to be shut down to the other cluster node prior to the shutdown. Perform the following steps:

1. To display the hostname of this node, enter **hostname** at the command prompt.
2. To display the group name of the volumes being served on this node, enter **clnasshowvol -a -n hostname**.

**Note:** Record both the host name and the group name.

3. Relocate the volumes to the other node in this cluster by entering **clnasrelocate -g group\_name -n new\_host\_name**.
4. Stop the cluster on the node being shut down by entering **cldisnode -n hostname**.

## Changing reboot options

You can specify whether the NAS Gateway 500 system software should reboot automatically after a system crash.

Specify whether the system should reboot after a system crash using the SMIT fastpath **smit chreboot**.

Whether the system does automatically reboot is also dependent on some Service Processor settings. Refer to the section entitled “Service Processor reboot/restart recovery” in the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*, SC30-4073.

---

## Setting the date and time

The system clock records the time of system events, allows you to schedule system events (such as running hardware diagnostics at 3:00 a.m.), and tells when you first created or last saved files. Use the **date** command to set your system clock. Some of the tasks you can perform to manage the system clock include:

- “Changing and showing date and time” on page 159
- “Changing the time zone” on page 159
- “Using the ntpq command” on page 160
- “Using the ntpdate command” on page 160

## Changing and showing date and time

The **date** command displays or sets the date and time.

The following formats can be used when setting the date with the date parameter:

- mmddHHMM[YYyy] (default)
- mmddHHMM[yy]

The variables to the date parameter are defined as follows:

- mm** Specifies the number of the month.
- dd** Specifies the number of the day in the month.
- HH** Specifies the hour in the day (using a 24-hour clock).
- MM** Specifies the minute number.
- YY** Specifies the first two digits of a four-digit year.
- yy** Specifies the last two numbers of the year.

A NAS Administrator can use the **date** command to set the current date and time. For example:

```
date 021714252002
```

sets the date to February 17, 2002, and the time to 14:25.

**Note:** Do not change the date when the system is running with more than one user.

For more information, refer to the **date** command in the *IBM TotalStorage NAS Gateway 500 Command Reference*.

### CLI command

At the command prompt, enter **date**.

### SMIT fastpath

The SMIT fastpath command to display the time or set the date is **smit date**.

### WebSM

In WebSM, use the following: **NAS Management**→**NAS System**→*Node*→**System Environment**→**Settings**, then double-click the **Date and Time** icon.

## Changing the time zone

The **chtz** command allows you to change the time zone for the system. By default, the **chtz** command uses the values for time zones located on the system. For more information, refer to the **chtz** command in the *IBM TotalStorage NAS Gateway 500 Command Reference*.

### CLI command

At the command prompt, enter **chtz TimeZoneInfo**.

### SMIT fastpath

The SMIT fastpath command to change time zone information is **smit chtz**.

The SMIT fastpath, **smit chtz\_user** allows you to specify the time zone and daylight savings information for the system.

## WebSM

In WebSM, do the following: **NAS Management** → **NAS System** → *Node* → **System Environment** → **Settings**, then double-click the **Date and Time** icon.

## Using the ntpq command

Use the **ntpq** command to start the standard Network Time Protocol (NTP) query program. The **ntpq** command queries the NTP servers running on the hosts. It runs either in interactive mode or by using command-line arguments. You can make requests to read and write arbitrary variables, and raw and formatted output options are available. The **ntpq** command can also obtain and print a list of peers in a common format by sending multiple queries to the server.

If you enter the **ntpq** command with one or more flags, the NTP servers running on each of the hosts specified (or defaults to local host) receive each request. If you do not enter any flags, the **ntpq** command tries to read commands from standard input and run them on the NTP server running on the first host specified or on the local host by default. It prompts for subcommands if standard input is the terminal.

For more information, refer to the **ntpq** command in the *IBM TotalStorage NAS Gateway 500 Command Reference*.

### CLI command

At the command prompt, enter **ntpq**.

## Using the ntpdate command

The **ntpdate** command sets the local date and time by polling the NTP servers specified to determine the correct time. It obtains a number of samples from each server specified and applies the standard NTP clock filter and selection algorithms to select the best of the samples.

For more information, refer to the **ntpdate** command in the *IBM TotalStorage NAS Gateway 500 Command Reference*.

### CLI command

At the command prompt, enter **ntpdate**.

---

## Problem determination

Diagnostic functions are:

- Displaying attributes of a dump, some of which can be changed. See “Changing dump options” on page 161.
- Gathering debugging data collects system debugging information. See “Gathering debugging data” on page 161.
- The hardware diagnostics function shuts down your system and puts it in the Maintenance Shell. This is a root user function only. See “Hardware diagnostics” on page 161.
- The trace facility allows you to monitor selected system events, including:
  - Entry and exit to selected subroutines
  - Kernel routines
  - Kernel extension routines
  - Interrupt handlers.

See “Tracing” on page 162.

## How to access diagnostic functions using NAS SMIT

To access the diagnostic functions, enter: **smit problems**.

The Problem Determination panel is displayed (see Figure 43).

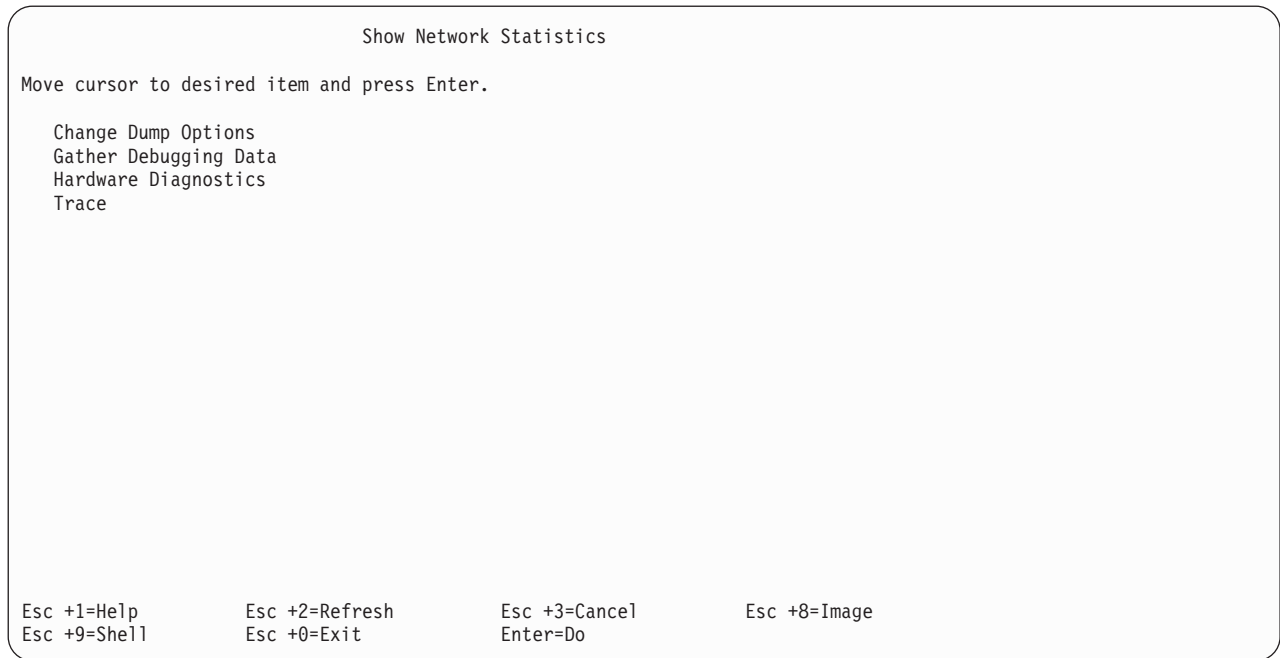


Figure 43. Example: Problem Determination panel

### Changing dump options

You can specify certain characteristics of system dumps that are taken including whether the dumps are allowed and whether dumps should be compressed.

You can specify dump-related settings using the SMIT fastpath **smit sysdumpdev**.

### Gathering debugging data

You can gather various system and configuration data to a file that then can be moved to disk or tape, or be transmitted to another system. This information may be needed to identify and resolve system problems.

**Note:** Any previously gathered debugging data is overwritten.

You can gather debugging data using the SMIT fastpath **smit snap**.

### Hardware diagnostics

The **diag** command is the starting point to run a wide choice of tasks and service aids that are used to perform hardware problem determination.

The **diag** command has a menu-driven interface, but can also be directed to perform specific tasks using command line flags.

Use the following steps to run diagnostics if you suspect a problem:

1. Run the **diag** command.
2. Press **Enter** to advance past the information screen.

3. Select **Diagnostic Routines**.
4. Select **Problem Determination**. This instructs the **diag** command to test the system and analyze the error log.

## Tracing

The **trace** command records selected system events that you specify. Facilities exist to:

- Start tracing
- Stop tracing
- Generate a trace report

Trace data is collected in a trace log from which a trace report can be created. The trace facility is only requested by the root user to assist in troubleshooting problems with your system. In this case, the root user supplies you with the values to be used in performing the trace and generating the trace report.

You can work the trace facility using the SMIT fastpath **smit trace**.

---

## System information

The NAS Gateway 500 system software includes several performance and diagnostic tools.

This section describes how to use performance and diagnostics tools.

### Displaying performance information

The performance information tools allow you to show:

- Command log - Displays a log that lists all commands that have been executed by the NAS administrator.
- CPU and I/O statistics - Displays statistics of CPU and I/O activities.
- File system performance - Displays information about the file system.
- Latest installed maintenance - Displays latest level of installed maintenance.
- NAS levels - Displays current version of NAS software and all associated components.
- Network statistics - Displays information about the network.
- NFS statistics - Displays information about NFS and RPC.
- Processes - Displays information on current processes running on your system.
- System activity - Displays activity currently running on your system.
- System uptime - Displays information about how long the system has been running.
- Virtual memory usage - Displays statistics about virtual memory usage.

#### How to access performance tools using NAS SMIT

To access the performance tools, enter: **smit sys\_info**.

The System Information panel is displayed (see Figure 44 on page 163).



```
System Information

Move cursor to desired item and press Enter.

Show Command Log
Show CPU and I/O Statistics
Show Filesystem Performance
Show Latest Installed Maintenance
Show NAS Levels
Show Network Statistics
Show NFS statistics
Show Processes
Show System Activity
Show System Uptime
Show Virtual Memory Usage

Esc +1=Help      Esc +2=Refresh      Esc +3=Cancel      Esc +8=Image
Esc +9=Shell     Esc +0=Exit         Enter=Do
```

Figure 44. Example: System performance information panel

## Displaying network information

The network information tools allow you to show the following network-related information:

- Clear statistics
- Buffer cache statistics
- Communication adapter statistics
- Interface state
- Memory management statistics
- Packet counts through communications subsystem
- Protocol statistics
- Routing tables
- Routing table statistics
- Sockets state

### How to access network information tools using NAS SMIT

To access the network information tools, enter: **smit show\_netstats**.

The Show Network Statistics panel is displayed (see Figure 45 on page 164).

### Show Network Statistics

Move cursor to desired item and press Enter.

- Clear Statistics
- Show Network Buffer Cache Statistics
- Show Network Communication Adapter Statistics
- Show Network Interface State
- Show Network Memory Management Statistics
- Show Network Packet Counts Through Communications Subsystem
- Show Network Protocol Statistics
- Show Network Routing Tables
- Show Network Routing Table Statistics
- Show Network Sockets State

Esc +1=Help  
Esc +9=Shell

Esc +2=Refresh  
Esc +0=Exit

Esc +3=Cancel  
Enter=Do

Esc +8=Image

*Figure 45. Example: Show Network Statistics panel*

---

## Chapter 29. Managing NAS volumes, Remote Mirrored systems, and snapshots

NAS volume management is a set of system software commands, shell script tools, and device drivers. It simplifies the management tasks for creating file shares with attached backend storage.

Using command syntax, the system software commands take a newly configured disk from external disk storage and create a mounted file system.

NAS volumes are only supported when they are created by NAS administrators. For more information, refer to the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.

Refer to the User's Guide that came with your storage subsystem for more information.

Before creating NAS volumes, ensure that you have completed the prerequisite steps as described in "Creating NAS volumes" on page 89.

This section contains the following subsections:

- "Managing NAS volumes"
- "Managing Remote Mirrored systems" on page 175
- "Managing snapshots" on page 178

---

### Managing NAS volumes

You can perform the following tasks to manage local volumes:

- "Configuring physical volumes" on page 166
- "Configuring NAS volumes" on page 166
- "Creating a NAS volume" on page 166
- "Changing a NAS volume" on page 167
- "Deleting a NAS volume" on page 167
- "Defragmenting a NAS volume" on page 168
- "Exporting a NAS volume" on page 168
- "Importing a NAS volume" on page 169
- "Extending the size of a NAS volume" on page 169
- "Copying a NAS volume" on page 169
- "Replacing a disk within a NAS volume" on page 170
- "Mounting a NAS volume" on page 170
- "Unmounting a NAS volume" on page 170
- "Creating a mirror of a local NAS volume" on page 171
- "Unmirroring a local NAS volume" on page 171
- "Synchronizing a NAS volume" on page 171
- "Listing NAS volumes in a system" on page 172
- "Viewing NAS volume statistics" on page 172

You can use the following tasks to manage remotely mirrored volumes:

- "Creating a remotely mirrored NAS volume" on page 173

- “Listing remotely mirrored NAS volumes” on page 173
- “Deleting a remotely mirrored NAS volume” on page 173
- “Extending the size of a remotely mirrored NAS volume” on page 174
- “Replacing a disk within a remotely mirrored NAS volume” on page 174
- “Viewing I/O statistics for a remotely mirrored NAS volume” on page 175

## Configuring physical volumes

After you define supported physical disks on your disk subsystem, use the **cfgmgr** command to make the supported physical disks known to the NAS Gateway 500 System Software. Use the NAS **lspvol** command to verify that the disks have been properly configured. This command shows all the disks that are configured in your NAS Gateway 500 system, the physical volume identifier (PVID), the NAS volume to which it belongs, and a description for each disk is also displayed.

## Configuring NAS volumes

The NAS Gateway 500 provides a wizard through WebSM for initial volume management configuration. Click the **WebSM** icon on your managing console. The WebSM main panel is displayed. From the navigation area, click **Volumes>Overview and Tasks>Create a NAS Volume**. The Welcome to the NAS Volumes Wizard panel is displayed. Read this panel and click the appropriate button at the bottom of the panel. Continue using the wizard, providing information where required, and clicking the button at the bottom of each panel. Each panel in this wizard contains instructions for completing the required information. Help is provided for some panels.

## Creating a NAS volume

After storage has been set up and allocated on external disk storage, a NAS volume can be created and configured for file serving. In a clustered system, a NAS volume is associated with a group on a node. To create a NAS volume, use the NAS command **mkvol**. This command uses the specified physical disks to create a NAS volume. A NAS volume can span across multiple disks. This allows you to create multiple volumes for multiple purposes, with varying storage sizes.

If the system has been configured for remote mirroring, the remote NAS volume can also be created at the time the local volume is being created. If snapshots will be remotely mirrored for this volume, select the proper option.

### CLI command

To create a volume with the CLI, use the **mkvol [ -r resource\_group ] [ -n num\_snapshots [ -s snapshot\_size ] ] [ -L ] volumename disk1 [ disk2 ... ] [ -g [ -c ] -X node\_name remote\_disk1 [ remote\_disk2... ] ]** command.

Parameter	Description
<b>-n</b> <i>num_snapshots</i>	Specifies the maximum number of snapshots that can be created for this volume. The default is 2.
<b>-r</b> <i>resource_group</i>	Specifies that the resource group identified by <i>resource_group</i> will own this NAS volume.
<b>-s</b> <i>snapshot_size</i>	Specifies the percentage of the file system space to be reserved for snapshots. The default value is 10%.
<b>-L</b>	Specifies the snapshot dynamic link management with default settings of the latest and previous snapshots linked.
<b>-g</b>	Specifies remote mirror copy creation.
<b>-c</b>	Specifies Remote Mirroring of snapshots.

Parameter	Description
<b>-X</b> <i>node_name</i>	Specifies the name of the node where the remote disks reside.

### SMIT fastpath

This command can be accessed through the SMIT fast path by executing **smit mkvol**. This displays all of the options that you can choose when creating a volume.

### WebSM

To create a volume using WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**Overview and Tasks**→**Create a NAS Volume**.

## Changing a NAS volume

Use the NAS command **chvol** if you want to rename your volume or perhaps change the owning group. This may be useful if the volume name represents the type of data that is to reside on the volume and the volume now contains a different type of data. Also, if you have two volumes that have a lot of activity being served from one group, you may want to move one to another group that does not have a lot of activity. This helps balance the load and increase performance.

**Note:** This command also applies to remotely mirrored volumes

### CLI command

To change the name of a volume, use the CLI command **chvol [ -n *new\_volumename* ] *volumename***.

To move the volume to another group, use the CLI command **chvol -r *resource\_group***.

Parameter	Description
<b>-n</b> <i>new_volumename</i>	Specifies that the name of the NAS volume identified by <i>volumename</i> is to be changed to the name specified by <i>new_volumename</i> .

### SMIT fastpath

To change the name of the volume with SMIT, use the **smit chvol** command.

### WebSM

To change a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ **(right-click a volume)** →**Change**.

## Deleting a NAS volume

Use the NAS command **rmvol** if you want to remove the NAS volume and all of its data from the system. The NAS volume is destroyed and the disks are released for use in other volumes. The file system and the snapshots are deleted.

If the system has been configured for remote mirroring, the remote NAS volume can also be deleted at the same time that the local volume is being deleted.

### CLI command

To delete a volume with the CLI, use the **rmvol [ -g ] [ -f ] *volumename*** command.

Parameter	Description
-f	If the mirror is present and active, this flag forces deletion of the mirror.
-g	Specifies that if there is a mirrored volume at the remote site that matches this volume, the mirrored volume should also be deleted.

### SMIT fastpath

To delete a volume with SMIT, use the **smit rmvol** command.

### WebSM

To delete a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Delete Volume**.

## Defragmenting a NAS volume

Use the NAS command **defragvol** when the file system associated with a NAS volume has been fragmented. You can use this command to increase contiguous free space within a volume and improve system performance. All snapshot schedules must be deactivated before using this command.

### CLI command

To defragment a volume with the CLI, use the **defragvol *volume\_name*** command.

### SMIT fastpath

To defragment a volume with SMIT, use the **smit defragvol** command.

### WebSM

To defragment a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Defragment**.

## Exporting a NAS volume

To remove the definition of a NAS volume from the system without destroying its data, use the NAS command **expvol**. This allows volume information to be retained on the disks so that it may be imported on another NAS Gateway 500 system or re-imported on the current system. This increases the portability of NAS volumes.

### CLI command

To export a volume with the CLI, use the **expvol [ -f ] *volumename*** command.

Parameter	Description
-f	If the mirror is present and active, this flag forces deletion of the mirror.

### SMIT fastpath

To export a volume with SMIT, use the **smit expvol** command.

### WebSM

To export a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Export**.

## Importing a NAS volume

Use the **impvol** command if you want to import an existing NAS volume into a system. You can specify a new name for the imported volume as well as the group that will own this volume. You can also choose whether or not the volume will be activated when it is imported.

### CLI command

To import a volume with the CLI, use the **impvol** `[-r group] [-v volume_name] [-a ] disk1` command.

### SMIT fastpath

To import a volume with SMIT, use the **smit impvol** command.

### WebSM

To import a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**Overview and Tasks**→**Import a NAS Volume**.

## Extending the size of a NAS volume

If you want to increase the size of your NAS volume's file system or change a snapshot parameter, use the **extendvol** command. There are two ways to increase the file system size:

1. Add additional disks.
2. Increase or decrease the percentage of the file system space reserved for snapshots and the number of snapshots that can be stored on the volume.

### CLI command

To extend a volume with the CLI, use the **extendvol** `[-R] [-n new_total_snapshots] [-s new_snapshot_percent] volumename [ disk1 [ disk2 ... ] ] [-g -X node_name [ remote_disk1 [ remote_disk2 ... ] ] ]` command.

Parameter	Description
<code>-n new_total_snapshots</code>	Specifies that the new maximum number of snapshots to be created is indicated by the value of <i>new_total_snapshots</i> .
<code>-R</code>	Specifies that the number of snapshots be reduced without increasing the size of the file system. This allows the existing snapshot schedule to migrate to the new size without causing any snapshots to be deleted.
<code>-s new_snapshot_percent</code>	Specifies that the percentage of the file system that snapshots will consume is indicated by <i>new_snapshot_percent</i> .
<code>-g</code>	Specifies that the size of the remotely mirrored volume should be extended using the physical <i>remote_disk1</i> and <i>remote_disk2</i> , ... on <i>node_name</i> .
<code>-X node_name</code>	Specifies the name of the node where the remote disks reside.

### SMIT fastpath

To extend the size of a volume with SMIT, use the **smit extendvol**.

### WebSM

To extend a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Extend**.

## Copying a NAS volume

Use the NAS command **cpvol** if you want to keep a copy of a NAS volume on a separate disk (or disks). This command copies all the contents of the specified

source volume to the specified destination volume. You can copy a NAS volume to another NAS volume on another system. You can even specify the path within the volume where you want the copy to reside.

**Note:** This copy will not be updated as a mirror would be. If you want a mirror copy, use **mirvol**.

### CLI command

To copy a volume with the CLI, use the **cpvol** [ **-S snapshot** ] *target\_volume* [*host\_name:destination\_volume/dir*] command.

### SMIT fastpath

To copy a volume with SMIT, use the **smit cpvol** command.

### WebSM

To copy a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Copy**.

## Replacing a disk within a NAS volume

If you have a disk failure and need to replace the bad disk with another disk, use the **replacevol** command. You can also use this command if you want to replace a small disk with a bigger disk, which would essentially increase the size of your NAS volume.

### CLI command

To replace a volume with the CLI, use the **replacevol** *volume\_name source\_disk destination\_disk* command.

### SMIT fastpath

To replace a volume with SMIT, use the **smit replacevol** command.

### WebSM

To replace a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Replace Disk**.

## Mounting a NAS volume

If a NAS volume has been unmounted, you can mount the volume using the **mountvol** command. This command makes the volume available to users.

**Note:** This function is not available in a clustered environment. For more information, see Chapter 23, “Managing clustered systems,” on page 109.

### CLI command

To mount a volume with the CLI, use the **mountvol** *volume\_name* command.

### SMIT fastpath

To mount a volume with SMIT, use the **smit mountvol** command.

### WebSM

To mount a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Mount**.

## Unmounting a NAS volume

If a NAS volume has been mounted, you can unmount the volume using the **unmountvol** command.



### CLI command

To unmount a volume with the CLI, use the **umountvol** *volume\_name* command.

### SMIT fastpath

To unmount a volume with SMIT, use the **smit umountvol** command.

### WebSM

To unmount a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Unmount**.

## Creating a mirror of a local NAS volume

To keep a mirrored copy of a volume on the local node in the case of a disk failure, use the **mirvol** command. This command allows the information on a NAS volume to be synchronized on another disk or set of disks. You can have up to two mirrored copies of a NAS volume (the original is the first copy).

**Note:** This command may take a long time to complete.

### CLI command

To mirror a volume with the CLI, use the **mirvol** *volume\_name disk1 [ disk2... ]* command.

### SMIT fastpath

To mirror a volume with SMIT, use the **smit mirvol** command.

### WebSM

To mirror a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→(right-click a volume)→**New**→**Remote Mirror Volume**.

## Unmirroring a local NAS volume

If it is unnecessary to keep a mirrored copy of a NAS volume on the local node, you can remove the mirrored copies. You can specify which mirror copy you would like to remove.

### CLI command

To unmirror a volume with the CLI, use the **mirvol -u** *volume\_name [mirror\_number]* command.

### SMIT fastpath

To unmirror a volume with SMIT, use the **smit unmirvol** command.

### WebSM

To unmirror a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Unmirror**.

## Synchronizing a NAS volume

If a mirrored copy of the volume is not current (that is, it is stale), use the **syncvol** command to update the mirrored copies and synchronize them with the original NAS volume.

**Note:** This command can take a long time to complete.

### CLI command

To synchronize a volume with the CLI, use the **syncvol** *volume\_name* command.

## SMIT fastpath

To synchronize a volume with SMIT, use the **smit syncvol** command.

## WebSM

To synchronize a volume in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Synchronize**.

## Listing NAS volumes in a system

To see all the volumes currently on a system, use the **lsvol** command. To view details for a specific volume, you can specify the volume name.

If the system has been configured for remote mirroring, the remote NAS volumes can also be listed at the same time that the local volumes are being listed.

### CLI command

To list a volume with the CLI, use the **lsvol** [ **-X** *node\_name* ] [ **-g** ] [ *volumename* ] command.

Parameter	Description
<b>-g</b>	Specifies that the information for the volume at the remote site should be listed.
<b>-X</b> <i>node_name</i>	Specifies the node name that the specified volume is on. The default is the local node.

## SMIT fastpath

To list a volume with SMIT, use the **smit lsvol** command.

To list a volume's attributes, use the **smit lsvolatt** command.

## WebSM

To list the volumes in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**List**.

## Viewing NAS volume statistics

To see reports of input/output statistics for a NAS volume, use the **volstat** command. You can use the information provided by these reports to better balance the input/output load between disks. You can also poll the volume to see the statistics during a specified interval.

If the system has been configured for remote mirroring, the remote NAS volume statistics can also be displayed from the local system.

### CLI command

To view the statistics with the CLI, use the

**volstat** [ **-X** *node\_name* ] [ **-g** ] *volumename* [ *interval* [ *count* ] ] command.

Parameter	Description
<b>-g</b>	Specifies that the volume is at the remote site.
<b>-X</b> <i>node_name</i>	Specifies that the node identified by <i>node_name</i> is the node for which information is to be displayed. The default is the local node.

## SMIT fastpath

To view the statistics with SMIT, use the **smit volstat** command.

## WebSM

To list the volumes statistics in WebSM, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Volumes**→ (right-click a volume) →**Statistics**.

## Creating a remotely mirrored NAS volume

If a NAS volume has already been created at the local site, you can create a remotely mirrored version of that NAS volume at a remote site that will mirror the local NAS volume. As long as the cluster is active, all data written to the local NAS volume will be mirrored over to the remote site.

### CLI command

At the command prompt, enter **mkgeovol** [ **-s** ] [ **-m** ] *volumename* **-X** *node\_name* *remote\_disk1* [ *remote\_disk2* ... ].

Parameter	Description
<b>-m</b>	Starts the mirror device after creating it. The default is to create the remote volume without starting the mirror.
<b>-s</b>	Specifies that snapshots should be mirrored remotely. If you do not specify <b>-s</b> , no snapshots are mirrored remotely.
<b>-X</b> <i>node_name</i>	Specifies the name of the node where the remote disks reside.

## SMIT fastpath

The SMIT fastpath command to remotely mirror a NAS volume is **smit mkgeovol**.

## WebSM

To remotely mirror a NAS volume from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Volumes**→**Overview and Tasks**→**Create a remote mirror volume**.

## Listing remotely mirrored NAS volumes

If the system has been configured for remote mirroring, you can list all of the remotely mirrored volumes currently on that remote system, by using the **lsvol** command. To view details for a specific volume, you can specify the volume name.

### CLI command

At the command prompt, enter **lsvol** [ **-n** *node\_name* ] *volumename*.

## SMIT fastpath

The SMIT fastpath command to list remotely mirrored NAS volumes is **smit lsvol**.

## WebSM

To list remotely mirrored NAS volumes from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Remote Mirror Volumes**→**List**.

## Deleting a remotely mirrored NAS volume

If the system has been configured for remote mirroring, you can remove remotely mirrored NAS volumes by using the **rmgeovol** command. This command removes NAS volumes only from the remote site. The local volumes are no longer remotely mirrored.

### CLI command

At the command prompt, enter **rmgeovol** *volumename*.

## SMIT fastpath

The SMIT fastpath command to delete a NAS volume at a remote site is **smit rmgeovol**.

## WebSM

To delete a NAS volume from a remote site, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Remote Mirror Volumes**→ (right-click a volume) →**Delete**.

## Extending the size of a remotely mirrored NAS volume

You can extend the size of a remotely mirrored NAS volume by using the **extendgeovol** command. This command takes a remotely mirrored NAS volume and increases the size.

### CLI command

At the command prompt, enter **extendgeovol** [ **-R** ] [ **-n** *new\_total\_snapshots* ] [ **-s** *new\_snapshot\_percent* ] *volumename* [ **-g** [ **-X** *node\_name* ] [ *remote\_disk1* [ *remote\_disk2* ... ] ] ].

Parameter	Description
<b>-R</b>	Specifies that the number of snapshots be reduced without increasing the size of the file system. This allows the existing snapshot schedule to migrate to the new size without causing any snapshots to be deleted.
<b>-n</b>	Specifies that the new maximum number of snapshots to be created is indicated by the value of <i>new_total_snapshots</i> .
<b>-s</b>	Specifies that the percentage of the file system that snapshots will consume is indicated by <i>new_snapshot_percent</i> .
<b>-g</b>	Specifies that the size of the remotely mirrored volume identified by <i>remote_disk1 remote_disk2 ...</i> should be extended. <b>-g</b> should be used only when you are logging on a node in the local site. If you are already logged in on a node at the remote site, <b>-g</b> should not be specified.
<b>-X</b> <i>node_name</i>	Specifies the name of the node where the remote disks reside.

## SMIT fastpath

The SMIT fastpath command to extend the size of a remotely mirrored NAS volume is **smit extendgeovol**.

## WebSM

To extend the size of a remotely mirrored NAS volume from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Remote Mirror Volumes**→ (right-click a volume) →**Extend**.

## Replacing a disk within a remotely mirrored NAS volume

To replace a disk within a remotely mirrored NAS volume, use the **replacegeovol** command. This command allows you to remove one disk from a volume, and replace it with another.

### CLI command

At the command prompt, enter **replacegeovol** *volumename node\_name remote\_sourcedisk destdisk*.

## SMIT fastpath

The SMIT fastpath command to replace a disk within a remotely mirrored NAS volume is **smit replacegeovol**.

### WebSM

To replace a disk within a remotely mirrored NAS volume from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Remote Mirror Volumes**→ (right-click a volume) →**Replace Disk**.

## Viewing I/O statistics for a remotely mirrored NAS volume

You can view I/O statistics for remotely mirrored NAS volumes.

### CLI command

At the command prompt, enter **volstat** [ *-n node\_name* ] *volumename* [ *interval* [ *count* ] ]

### SMIT fastpath

The SMIT fastpath command to view I/O statistics for remotely mirrored NAS volumes is **smit volstat**.

### WebSM

To view I/O statistics for remotely mirrored NAS volume from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Volumes**→**All Remote Mirror Volumes**→ (right-click a volume) →**Statistics**.

## Clearing NAS information from a remote disk

You can clear NAS information from a remote disk.

### CLI command

At the command prompt, enter **chpgeovol -C** *node\_name remote\_hdisk*.

### SMIT fastpath

The SMIT fastpath command to clear NAS information is **smit chpgeovol**.

### WebSM

Not applicable

---

## Managing Remote Mirrored systems

Use the following tasks to manage Remote Mirrored systems:

- “Starting a mirror”
- “Stopping a mirror” on page 176
- “Listing mirrors” on page 176
- “Viewing mirror log files” on page 176
- “Taking mirror snapshots” on page 177
- “Listing mirror snapshots” on page 177
- “Restoring mirrors from a snapshot” on page 178

## Starting a mirror

You can start mirroring on one or more volumes.

### CLI command

From the command line, enter

```
startmirror -d {ALL | devicename [ devicename... ] }
```

where *devicename* specifies the mirror or mirrors to start. The keyword ALL specifies that all mirror devices should be started.

### SMIT fastpath

The SMIT fastpath command to start a mirror is **smit startmirror**.

### WebSM

To start a mirror from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**All Remote Mirror Devices**→(right-click a remote device)→**Start** .

## Stopping a mirror

You can stop mirroring on one or more volumes without deleting the volume or the remote mirroring configuration.

**Note:** This command can be used when a situation at one site would affect a remote copy of the volume that is being mirrored. Stopping the mirroring can prevent some performance problems associated with a remote volume being inaccessible. When the remote copy becomes available, the **startmirror** command must be used to restart mirroring to synchronize the two copies. Failure to use the **startmirror** command to restart the mirroring can result in data integrity problems.

### CLI command

From the command line, enter **stopmirror -d {ALL | *devicename* [ *devicename* ...] }** where *devicename* specifies the volume or volumes to stop. The keyword ALL specifies that all mirror devices should be stopped.

### SMIT fastpath

The SMIT fastpath command to stop a mirror is **smit stopmirror**.

### WebSM

To stop a mirror from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**All Remote Mirror Devices**→(right-click a remote device)→**Stop** .

## Listing mirrors

You can list all of the remotely mirrored volumes.

### CLI command

From the command line, enter **lsmirror**.

### SMIT fastpath

The SMIT fastpath command to list a mirror is **smit lsmirror**.

### WebSM

To list a mirror from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**All Remote Mirror Devices**→(right-click a remote mirror device)→**Properties**.

## Viewing mirror log files

You can display the Remote Mirroring log or statistical information regarding remotely mirrored volumes.

### CLI command

From the command line, enter **geonasviewlog** *logname*, where *logname* is the type of log to be displayed. Valid values are:

- **nasxd** – contains the actions that have occurred on a mirrored device, including the steps required to make, change, remove, start, or stop a mirrored volume
- **krpc\_log** – contains statistical data regarding remote clustering operations, such as network information
- **gmd\_log** – contains statistical data regarding the remote mirrored devices, such as bytes read or written for the local and remote sites

### SMIT fastpath

The SMIT fastpath command to view a mirror log is **smit geonasviewlog**.

### WebSM

To view a mirror log from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**Overview and Tasks**→**View Remote Mirroring logs**.

## Taking mirror snapshots

Mirror snapshots are backups of configuration information for all the mirrored devices. Taking a snapshot is used to save the configuration information for the remotely mirrored volumes that are currently configured. This configuration information can be easily restored by following the procedure “Restoring mirrors from a snapshot” on page 178.

You can create a snapshot of the Remotely Mirrored volumes.

### CLI command

From the command line, enter **geo\_snapshot -t -f <snapshot\_file>**.

### SMIT fastpath

The SMIT fastpath command to create a snapshot of the mirrors is **smit geo\_snapshot**.

### WebSM

To create a snapshot of the mirrors from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**Overview and Tasks**→**Create a snapshot of all remote mirroring devices**.

## Listing mirror snapshots

You can list the backups of configuration information for all the remotely mirrored volumes.

### CLI command

From the command line, enter **geo\_snapshot -l**.

### SMIT fastpath

The SMIT fastpath command to list the mirror snapshots is **smit geo\_snapshot**.

### WebSM

To list mirror snapshots from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Remote Mirroring**→**Overview and Tasks**→**List Snapshots of Remote Mirror Devices**.

## Restoring mirrors from a snapshot

You can restore the configuration information for all the remotely mirrored volumes, if, for example, the software or the whole system, needs to be reinstalled.

### CLI command

From the command line, enter **geo\_snapshot -a -f <snapshot\_file>**.

### SMIT fastpath

The SMIT fastpath command to restore from a snapshot of the mirrors is **smit geo\_snapshot**.

### WebSM

To restore from a snapshot of the mirrors from the main WebSM panel, navigate to: **NAS Management→NAS System→Remote Mirroring→Overview and Tasks→Apply a snapshot of the remote mirroring devices to the system**.

---

## Managing snapshots

The NAS volume snapshot captures a consistent block-level image of a volume at any given point in time. The snapshot remains the same even if the source volume changes. The snapshot can then be used to create a backup of the volume. The snapshot also provides the capability to access files or directories as they were at the time of the snapshot. The snapshot can be generally viewed as a mechanism of backing up a specific NAS volume.

**Note:** A snapshot needs approximately two to six percent of the space needed for the volume that the snapshot was taken from. In the case of a highly active snapped volume, this estimate could rise to 15 percent.

You can perform the following tasks when working with snapshots:

- “Creating a snapshot”
- “Deleting a snapshot” on page 179
- “Renaming a snapshot” on page 179
- “Rolling back a snapshot” on page 180
- “Showing all current snapshots” on page 180
- “Configuring a snapshot schedule” on page 181
- “Managing a snapshot schedule” on page 182
- “Showing a snapshot schedule” on page 182
- “Snapshot Link Management” on page 183

## Creating a snapshot

The **snapvol -C** command creates a snapshot. If you specified that snapshots should be mirrored when you created the remotely mirrored NAS volumes, this snapshot will also be remotely mirrored,

Use one of the following interfaces to create a snapshot.

### Notes:

1. If you reach the maximum number of snapshots for a particular volume, more snapshots can be added through the **extendvol** command (see “Extending the size of a NAS volume” on page 169).
2. Within a cluster configuration, the cluster must be started to allow volumes to be mounted. Unmounted volumes will not be in the list for creating snapshots.



**Note:**

### CLI command

To create a snapshot, enter the **snapvol -C** *volume\_name snapshot\_name* command, where:

*volume\_name*

The name of the volume that is to be copied.

*snapshot\_name*

The name to be used for the snapshot.

### SMIT fastpath

The SMIT menu fastpath command to create a snapshot is **smit snapshot**.

To use the SMIT interface to create a snapshot using the SMIT fastpath, enter **smit snapvolC**. The options that can be chosen when creating a snapshot are displayed.

### WebSM

To create a snapshot from the main WebSM panel, navigate to: **NAS Management→NAS System→Snapshots→Overview and Tasks→Create a Snapshot**. This starts a series of dialog boxes that you can use to create a snapshot.

## Deleting a snapshot

You can remove a snapshot from a NAS volume. This command deletes the snapshot and unmounts it. This command will also delete the mirrored copies of the snapshot.

Use one of the following user interfaces to delete a snapshot:

### CLI command

To delete a snapshot, use the **snapvol -R** *volume\_name snapshot\_name* command, where

*volume\_name*

The name of the volume whose snapshot is to be deleted.

*snapshot\_name*

The name of the snapshot to be deleted.

### SMIT fastpath

The SMIT menu fastpath command to delete a snapshot is **smit snapvolR**.

### WebSM

To delete a snapshot from the main WebSM panel, navigate to: **NAS Management→NAS System→Snapshots→All Snapshots→(right-click a snapshot)Delete**.

## Renaming a snapshot

You can rename a snapshot or change the owning volume. This can be useful if you want to save older versions of a particular snapshot on another volume for later use. This command will also rename the mirrored copy of the snapshot.

Use one of the following interfaces to rename a snapshot:

### CLI command

To rename a snapshot, use the **snapvol -N** *volume\_name snapshot\_name* command, where

*volume\_name*

The name of the volume whose snapshot is to be renamed.

*snapshot\_name*

The name of the snapshot to be renamed.

### SMIT fastpath

The SMIT menu fastpath command to rename a snapshot is **smit snapvolN**.

### WebSM

To rename a snapshot from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Snapshots**→**All Snapshots**→(right-click a snapshot)Rename.

## Rolling back a snapshot

You can restore the file system to a particular point in time when a snapshot was taken.

Use one of the following user interfaces to roll back a snapshot:

### CLI command

To roll back a snapshot, use the **snapvol -r** *volume\_name snapshot [ rolledback\_pathname ]* command.

*volume\_name*

The name of the volume whose snapshot is to be renamed.

*snapshot*

The name of the snapshot to be renamed.

*rolledback\_pathname*

Specifies the path where the snapshot is to be recovered to.

### SMIT fastpath

The SMIT menu fastpath command to roll back a snapshot is **smit snapvolr**.

### WebSM

To roll back a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Snapshots**→**All Snapshots**→(right-click a snapshot)Rollback.

## Showing all current snapshots

You can display all the snapshots currently on a volume. A single line of status information is displayed for each snapshot in the system. When a volume name is used with this action, a portion of the volume information is also displayed.

Use one of the following user interfaces to show all current snapshots:

### CLI command

To show all current snapshots, use the **snapvol -L** *volume\_name* command.

*volume\_name*

The name of the volume whose snapshot is to be shown.

## SMIT fastpath

The SMIT menu fastpath command to show all current snapshots is **smit snapvol**.

## WebSM

To show all current snapshots from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Snapshots**→**All Snapshots**→**Show All**.

## Configuring a snapshot schedule

You can create a snapshot at a specified time or after a particular action takes place on a recurring basis. You can take individual snapshots at specific times even if no one is available to administer the NAS 500 Gateway. You can take monthly, weekly, daily, or hourly snapshots. This command also has the capability of calling a separate backup command to back up the newly created snapshot immediately to a specified location in storage and then delete it.

**Note:** Once the maximum number of snapshots has been created during a snapshot schedule, each subsequent snapshot created replaces the earliest-created snapshot. (For example, if three snapshots were specified as the maximum and three scheduled snapshots have been taken, the fourth scheduled snapshot created replaces the first snapshot of the original three.)

Use one of the following user interfaces to configure a snapshot schedule:

### CLI command

To configure a snapshot schedule, use the **snapvol [ -Y volume\_name { -c backup\_command | -D duration | -m month | -w weekday | -h hour } ]** command.

#### Operations flags

<b>-Y</b>	Creates a snapshot schedule for the specified NAS volume.
<b>-c</b>	Provides a <i>backup_command</i> to make a backup for an automatically scheduled snapshot.
<b>-D</b>	Specifies the <i>duration</i> (number of days) that this snapshot is to be active. This is available only for weekly and monthly snapshots.
<b>-m</b>	Specifies the day of the <i>month</i> that the snapshot is scheduled. The default is the first day of the month.
<b>-w</b>	Specifies the day of the <i>week</i> that the snapshot is scheduled. The default is Sunday.
<b>-d</b>	Specifies the days of the week that the snapshot is scheduled. The default is all the days of the week.
<b>-h</b>	Specifies the time that the snapshot is scheduled. The default is every hour between 8 and 17.

## SMIT fastpath

The SMIT menu fastpath command to configure a snapshot schedule is **smit snapvol**.

## WebSM

To configure a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS System**→**Snapshots**→**Overview and Tasks**→**Configure a Snapshot**.

## Managing a snapshot schedule

After a snapshot schedule has been created, the schedule can be managed. These commands allow you to stop a volume snapshot schedule, activate a volume snapshot schedule, and delete a volume snapshot schedule.

Use one of the following user interfaces to manage a snapshot schedule:

### CLI command

To stop a snapshot schedule, use the **snapvol -S** *volume\_name* command. This command stops a volume snapshot schedule until the schedule is reactivated, so no future snapshots are taken when the scheduled time arrives.

To activate a stopped snapshot schedule, use the **snapvol -A** *volume\_name* command.

To delete a snapshot schedule, use the **snapvol -X** *volume\_name* command.

*Volume\_name* is the name of the volume whose schedule you want to manage.

### SMIT fastpath

The SMIT menu fastpath command to stop a snapshot schedule is **smit snapvolS**.

The SMIT menu fastpath command to activate a stopped snapshot schedule is **smit snapvolA**.

The SMIT menu fastpath command to delete a snapshot schedule is **smit snapvolX**.

### WebSM

To create a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS system**→**Snapshots**→**All Snapshots**→(right-click the volume)→**Stop Schedule**.

To activate a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS system**→**Snapshots**→**All Snapshots**→(right-click the volume)→**Activate Schedule**.

To delete a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS system**→**Snapshots**→**All Snapshots**→(right-click the volume)→**Delete Schedule**.

## Showing a snapshot schedule

After a snapshot schedule or multiple snapshot schedules have been created, you can list all scheduled snapshots. This shows all scheduled snapshots whether or not they have been deactivated.

Use one of the following user interfaces to show a snapshot schedule.

### CLI command

To show a snapshot schedule, use the **snapvol -I** *volume\_name* command.

*Volume\_name* is the name of the volume whose snapshot schedule is to be displayed.

## SMIT fastpath

The SMIT menu fastpath command to show a snapshot schedule is **smit snapvoll**.

## WebSM

To show a snapshot schedule from the main WebSM panel, navigate to: **NAS Management**→**NAS system**→**Snapshots**→**All Snapshots**→(right-click the volume)→**Show Schedule**.

## Snapshot Link Management

Snapshot Link Management (SnapLM) enables you to automatically access snapshots through links that are created based on snapshot age and optional static link definitions. The exported snapshot links allow you to mount the latest snapshot, the previous snapshot, and, also, a statically-defined snapshot. The NAS Gateway 500 can refresh its mounts manually on demand, or it can refresh the mounts using a simple script that runs on a schedule synchronized with the snapshot schedule. Once the mount is refreshed, SnapLM ensures that the snapshot you reference is the one you want.

### SnapLM commands

**snaplmon:** The **snaplmon** command allows you to choose settings for snapshot link management for the desired volume. Valid variables are:

- -l (latest only)
- -s snapshot\_name (static only)
- -l -p (latest and previous)
- -l -s snapshot\_name (latest and static)
- -l -p -s snapshot\_name (latest, previous, and static)

Examples of the **snaplmon** command are:

- **snaplmon vol2 -l** (create a link to the latest snapshot on vol2)
- **snaplmon vol3** (create links for vol3 using defaults)

**snaplmo:** This command disables snapshot link management for the desired volume. All settings to create links for the volume are cleared, and the defined symbolic links are deleted. No actual snapshot data is affected, and snapshots that were exported by following the symbolic links are still available through NFS using their actual path names.

An example of the **snaplmo** command is: **snaplmo vol2** (disable snapshot link management on vol2)

**snaplm:** This command creates and updates links for the desired volume. This command reads the settings created by **snaplmon**, and then takes appropriate action to create or update symbolic links to the volume's snapshots. After the updates take place, the snapshot links are re-exported. The **snaplm** command is rarely called directly by the administrator. It is automatically invoked by **snaplmon**, and the **snapvol** create, delete, and rename commands.

**mkvol -L:** The **mkvol -L** command allows a volume to enable snapshot link management at creation. An example of **mkvol** is: **mkvol -n 8 -s 20 -L vol8 hdisk8** (create a NAS volume vol8 on hdisk8 with 20% of the volume reserved for a maximum of eight snapshots with SnapLM on).

## Automating SnapLM

This section contains information on automating SnapLM on both the NAS Gateway 500 and the attached NFS clients.

### ***NAS Gateway 500:***

1. Determine what type of snapshot linking you want (latest, previous, static, or a combination) .
2. Enable SnapLM for an existing volume with **snaplmon** or at volume creation with **mkvol -L**.
3. Create snapshots manually or create and enable a snapshot schedule.
4. SnapLM automatically generates the desired links.
5. Define NFS exports for snapshot links with **mknasnfsexp** or **smit nfs** as the NAS administrator user.

### ***Attached NFS clients:***

1. Create mount points for snapshot links.
2. Create a script that unmounts and remounts snapshot links.
3. Edit the crontab to run the mounting script at a time that synchronizes with the snapshot schedule.

---

## Part 5. Advanced management topics

This section contains additional configuration and management advanced topics to be performed by the root user.

**Note:** The task descriptions assume that you are logged in to the NAS Gateway 500 system as root. When you are directed to log in as root (and are not performing initial configuration), log in as a NAS administrator and use the **maintshell** command to gain root authority.

This section contains the following chapters:

- Chapter 30, “System backup and recovery,” on page 187 describes backup and recovery tasks.
- Chapter 31, “Call home,” on page 195 describes use of the Electronic Service Agent™™ for monitoring critical components.
- Chapter 32, “Inventory Scout,” on page 239 describes the use of Inventory Scout to collect the NAS Gateway 500’s vital product data (VPD) and transmit this information, through the Electronic Service Agent (ESA) to IBM for matching with a Miscellaneous Equipment Specification (MES) upgrade.
- Chapter 33, “Uninterruptible power supply,” on page 241 describes use of an external uninterruptible power supply (UPS) for your NAS Gateway 500.
- Chapter 34, “System upgrades and configuration changes,” on page 243 describes how to upgrade the system hardware and software by ordering additional features.
- Chapter 35, “Miscellaneous administration tasks,” on page 251 describes miscellaneous administration and integration tasks.





---

## Chapter 30. System backup and recovery

**Attention:** Changing the preloaded software configuration of this product, including applying or installing unauthorized service packs or updates to preinstalled software, or installing additional unsupported software products that are not included in the preloaded image, or on the Supplementary CD-ROM might not be supported and could cause unpredictable results. For updated compatibility information, visit the following Web site:

<http://www.ibm.com/servers/storage/support/>

To correct problems with preloaded software components, back up your user and system data. Then, use the NAS Gateway 500 System Software Recovery CD-ROM set to restore the preloaded software image to its original state.

The NAS Gateway 500 provides several means for system recovery, such as system snapshot, TSM, and the **mksysb** and **mknasb** commands. Depending on the environment and requirements the system administrator should use **mksysb** or TSM in their periodic maintenance operations for system recovery. This section provides details in using the **mksysb** for creating a system backup for the NAS Gateway 500 System Software.

---

### Save or restore hardware management policies

To reach this service aid, enter the **diag** command using the CLI, and then select the **Task Selection option** from the FUNCTION SELECTION menu.

Use this service aid to save or restore the Service Processor settings such as Ring Indicate Power-On Policy, Surveillance Policy, Remote Maintenance Policy and Reboot Policy. The following options are available:

- Save Hardware Management Policies  
This selection writes all of the settings for the hardware-management policies to the following file: **/etc/lpp/diagnostics/data/hmpolicies**.
- Restore Hardware Management Policies  
This selection restores all of the settings for the hardware-management policies from the contents of the following file: **/etc/lpp/diagnostics/data/hmpolicies**.

You can access this service aid directly from the command line, by typing:

```
/usr/lpp/diagnostics/bin/uspchrp -a
```

---

### System recovery using mksysb

A system backup is a copy of the root volume group (rootvg) of your system and is often referred to as a **mksysb**, in reference to the command used to create the system backup. The root volume group contains the following:

- Startup commands
- Base operating system commands and files
- System configuration information
- Optional software products

The **mksysb** backs up all JFS2 (Enhanced Journaled File Systems) mounts in the **rootvg** Volume group. Paging space and logical volume information are saved so

that the rootvg will be recreated. If there are JFS2 file systems that are not to be backed up, you can use an exclude list or you can unmount them before the backup is made.

The following table describes the methods you can use to back up a system.

Table 5. System backup methods

Backup Method	Considerations
NIM	Allows fast backup and recovery of a system. Because all images are backed up to one location (the NIM master), you should also back up your system and images to other physical media (tape, CD-RW, DVD-RAM).
<b>mksysb</b> command with a tape device	Creates a bootable backup. Must boot from CD or tape to reinstall. Remote tape drives are supported with Sysback (for more information, see <a href="http://sysback.services.ibm.com">http://sysback.services.ibm.com</a> ).

---

## Creating a system backup

You can create a system backup by using one of the following methods:

### Using NIM

With the NIM environment, you can create a system backup that is a selectable resource. That selectable resource can be used to reinstall the system on which it was created, or it can be cloned to another system. Because of its flexibility, NIM is the recommended method to back up and reinstall your systems (provided a NIM master is already available).

To use NIM to create a system backup, do the following:

1. If your systems were installed with NIM, go to Step 5.
2. On your NIM master, to determine whether your system is already defined as a NIM client, type:
 

```
# lsnim -t standalone
```
3. If the target system is not already a NIM client, configure it by running the following on the target system:
 

```
# smitty nimit
```
4. On your NIM master, run the following to define the target system (the system to be backed up) as a NIM client:
 

```
# smitty nim_mkmac
```
5. On your NIM master, type the following to open the Define a Resource menu:
 

```
# smitty nim_mkres
```
6. Select **mksysb** and type the appropriate information. This menu defines the **mksysb** resource and also creates the system backup image.

**Note:** Be sure to change the *CREATE system backup image?* selection to yes.

```

                                Define a Resource

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* Resource Name                 [P1_backup]
* Resource Type                 mksysb
* Server of Resource            [master]
* Location of Resource          [ /export/nim/mksysb/P1_backup]
  Comments                      []

Source for Replication          []
  -OR-

System Backup Image Creation Options:
  CREATE system backup image?   yes
  NIM CLIENT to backup          [system1]
  PREVIEW only?                 no
  IGNORE space requirements?    no
  EXPAND /tmp if needed?        no
  Create MAP files?             no
  Number of BLOCKS to write in a single output
  (leave blank to use system default)  []
  Use local EXCLUDE file?       no
  (specify no to include all files in backup)
  -OR-
  EXCLUDE_FILES resource        []
  (leave blank to include all files in backup)

```

## Backing up to tape media or a file

**mksysb** provides the capabilities to backup the NAS Gateway 500 System Software directly to some attached tape media or directly to a file. This can be accomplished using SMIT or through the Command Line Interface.

```

                                Backup the System

Type or select valules in entry fields.
PressEnter AFTER making all desired changes.

                                [Entry fields]
WARNING:  Execution of the mksysb command will
          result in the loss of all material
          previously stored on the selected
          output medium. This command backs
          up only rootvg volume groups.

* Backup DEVICE or FILE        [ ]          +/
  Create MAP files?            no           +
  List files as they are backed up?  no       +
  Verify readability if tape device? no       +
  EXPAND /tmp if needed?        no         +
  Disable software packing of backup? no       +
  Number of BLOCKS to write a single output
  (Leave blank to use a system default) [ ]      #

Esc+1=Help      Esc+2=Refresh      Esc+3=Cancel      Esc + 4 =List
Esc+5=Reset     Esc+6=Command      Esc+7=Edit        Esc + 8 =Image
Esc+9=Shell     Esc+0=Exit        Enter=Do

```

1. Enter the `smit mksysb` fast path.
2. Select the tape device in the Backup **DEVICE** or **FILE** field.
3. If you want to create map files, select **yes** in the **Create Map Files?** field.
4. To exclude certain files from the backup, select **yes** in the **Exclude Files** field.
5. Select **yes** in the List files as they are backed up field.
6. Use the default values for the rest of the menu options.
7. Press **Enter** to confirm and begin the system backup process.
8. The Command Status panel displays, showing status messages while the system makes the backup image. When the backup process finishes, the **COMMAND:** field changes to **OK**.
9. To exit SMIT when the backup completes, press **Esc+0**.
10. Remove the tape and label it. Write-protect the backup tape.
11. Record any backed-up root and user passwords. Remember that these passwords become active if you use the backup to either restore this system or install another system.

---

## Installing a system backup using NIM

You can use the NIM environment to install a system backup onto one or more of your systems. NIM is recommended because of its flexibility and customizing options for installation and system management. Also, NIM allows for multiple installations at the same time.

Before you can use NIM to install a system backup, make sure that the following conditions are met:

- Your network environment must be working correctly. The NIM master must be configured correctly, and the `lpp_source`, `SPOT`, and **mksysb** resources must be defined.
  - The target systems might not contain the same hardware devices or adapters. If this is the case, then the **mksysb**, `SPOT`, and `lpp_source` resources will be needed to install the needed device support.
  - Because NIM configures TCP/IP at the end of an installation, it is recommended that a `bosinst_data` resource be allocated for cloning **mksysb** installations with the `RECOVER_DEVICES` field set to *no*. This action prevents the BOS installation process from attempting to configure the devices as they were on the source machine of the **mksysb**.
1. To use a **mksysb** resource to install a NIM client, enter the `smit nim_bosinst` fast path.
  2. Select a target for the operation.

Select a TARGET for the operation

Move cursor to desired item and press Enter.

lpar1	machines	standalone
lpar2	machines	standalone
lpar3	machines	standalone

3. Select `mksysb` as the installation **TYPE**.
4. Select the `mksysb` to use for the installation.
5. Select the `SPOT` to use for the installation.

6. The Install the Base Operating System on Standalone Clients panel looks similar to the following:

```
Install the Base Operating System on Standalone Clients

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]
* Installation Target          [Entry Fields]
* Installation TYPE           1par1
* SPOT                        mksysb
LPP_SOURCE                    520spot_res
MKSYSB                         []
BOSINST_DATA to use during installation 520mksysb
IMAGE_DATA to use during installation  []
RESOLV_CONF to use for network configuration []
Customization SCRIPT to run after installation []
Customization FB Script to run at first reboot []
ACCEPT new license agreements? [no]
Remain NIM client after install? [yes]
[MORE...35]
```

7. Select a bosinst\_data resource to perform a non-prompted installation. Select the **bosinst\_ow** resource for a new and complete overwrite installation.
8. Select a resolv\_conf resource to establish network configuration for the client system.
9. Set the Accept new License Agreements field to yes.

The Install the Base Operating System on Standalone Clients menu looks similar to the following:

## Install the Base Operating System on Standalone Clients

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

```
[TOP]                                [Entry Fields]
* Installation Target                 1par1
* Installation TYPE                   mksysb
* SPOT                                520spot_res
  LPP_SOURCE                           []
  MKSYSB                                520mksysb

  BOSINST_DATA to use during installation [bosinst_ow]      +
  IMAGE_DATA to use during installation  []
  RESOLV_CONF to use for network configuration [resolv_res]    +
  Customization SCRIPT to run after installation []
  Customization FB Script to run at first reboot []
  ACCEPT new license agreements?         [yes]
  Remain NIM client after install?       [yes]
  PRESERVE NIM definitions for resources on this target? [yes]
  FORCE PUSH the installation?             [no]

  Initiate reboot and installation now?   [yes]
  -OR-
  Set bootlist for installation at the next reboot? [no]

  Additional BUNDLES to install           []
  -OR-
  Additional FILESETS to install         []
  (bundles will be ignored)

[MORE...20]
```

10. Press **Enter** to install the NIM client.
11. If the client system being installed is not already a running, configured NIM client, NIM will not automatically reboot the machine over the network for installation. If the client was not rebooted automatically from SMIT, initiate a network boot from the client to install it.

---

## Installing a system backup using a tape device

This section describes how to use a tape device to install a system backup onto one or more of your systems.

**Note:** Do not use SMIT to restore from a tape device.

The following procedure is the only procedure supported by the NAS Gateway 500 for installing a system backup using a tape device. It requires a console attached to serial port 1. For information on console strategy, refer to the *IBM TotalStorage NAS Gateway 500 Service Guide*.

1. Boot the system with the NAS Gateway 500 System Software Recovery disk 1 CD in the CD-ROM drive and the system backup tape in the tape device by following these steps:
  - a. Power the system on.
  - b. Immediately insert the NAS Gateway 500 System Software Recovery disk 1 CD into the CD-ROM device.

- c. When the keyboard indicator is shown on the screen (the word keyboard on the console), press **5** on the console. This will temporarily alter the boot list.
  - d. At this stage, the system boots up using the media. If the system does not boot up, but instead enters SMS, there is a problem with the media. Verify that it is correctly inserted and undamaged. Reinsert the media or replace the media and restart at Step 1.
2. After the machine boots up, follow the instructions that are displayed on the panel.
  3. Select **Start Maintenance Mode for System Recovery**.
  4. Select **Install from a System Backup**.
  5. Select the drive containing the backup tape and press **Enter**.

The system reads the media and begins the installation. If the mksysb is saved on multiple tape cassettes, you will be prompted to insert the next cassette during the installation. You are then prompted for the BOS installation language.

During a restore of a tape backup, do not remove the CD-ROM from the CD-ROM drive. After the mksysb installation completes, the installation program automatically installs additional devices and the kernel on your system, using the original product media that you booted from.

---

## Using the System Software Recovery CD-ROM

This section describes how to use the recovery CD-ROMs you received in the NAS Gateway 500 software ship group. These CD-ROMs contain the preload image of the system software installed during manufacturing and are used to reconfigure the NAS Gateway 500 back to the manufacturing state.

**Attention:** Installing the recovery image will erase ALL data on the system disks.

**Note:** This process requires *root* authority and a console attached to serial port 1. For information on console strategy, refer to the *IBM TotalStorage NAS Gateway 500 Service Guide*.

To start the installation of the NAS Gateway 500 recovery image, your system needs to first boot from the NAS Gateway 500 System Software Recovery CD-ROM. In order to force a boot from the media:

### If the system is powered on:

1. Run the following commands
 

```
bootlist -m normal cd0 hdisk0
shutdown -Fr
```
2. The system will shutdown and boot off the media in the CD-ROM drive.
3. After the machine boots up, follow the instructions that are displayed on the screen.
4. Choose the terminal that you will be using.
5. Select the language.
6. Click **Start Install Now** with default settings.
7. Click **Continue with Install**.
8. The system will load the image. When the System Software Recovery CD-ROM disk 1 is complete, it will prompt you to insert System Software Recovery CD-ROM disk 2.

9. After the install is complete, the system will reboot automatically.

**If the system is powered off:**

1. Power the system on.
2. Immediately insert the NAS Gateway 500 System Software Recovery CD-ROM disk 1 into the CD-ROM device.
3. When the keyboard indicator is shown on the screen (the word *keyboard* on the console), press **5** on the console. This will temporarily alter the boot list.
4. At this stage, the system boots up using the media. If the system does not boot up but instead enters SMS, there is a problem with the media. Check if it is correctly inserted and undamaged. Reinsert the media or replace the media and restart at Step 1.
5. After the machine boots up, follow the instructions that are displayed on the screen.
6. Select the terminal that you will be using.
7. Select the language.
8. Click **Start** Install Now with default settings.
9. Click **Continue** with Install.
10. The system loads the image. When System Software Recovery CD-ROM disk 1 is complete it prompts you to insert System Software Recovery CD-ROM disk 2.
11. After the install is complete, the system reboots automatically.



---

## Chapter 31. Call home

**Note:** Some menu screens contain options that you cannot use with the NAS Gateway 500. These options appear because they are used by other IBM products which share the same menus. Notes in each section tell you which options are invalid.

The NAS Gateway 500 allows you to use the Electronic Service Agent to monitor critical components. When error events occur, notifications can be sent to monitoring facilities.

The IBM Electronic Service Agent is an application on the HDD, ready for installation on your NAS Gateway 500, that is designed to monitor events proactively and transmit system inventory information to IBM on a periodic customer-defined timetable. The IBM Electronic Service Agent is able to track system inventory and hardware error logs as well as provide automatic error reporting and analysis without customer intervention.

Early knowledge about potential problems enables IBM to provide proactive service that maintains higher system availability and performance. In addition, information collected through the Electronic Service Agent will be made available to IBM service representatives when they are helping answer your questions or diagnosing problems.

---

### Electronic Service Agent introduction

This section describes the Electronic Service Agent for the NAS Gateway 500.

**Notes:**

1. Root access is required to enable and configure the Electronic Service Agent.
2. For IBM to service a machine or machines, each machine must be under a warranty or maintenance agreement (MA), and must be verified with IBM entitlement checking. Only those NAS Gateway 500s on an IBM Warranty or maintenance agreement (MA) can use Electronic Service Agent to report errors to IBM. If the NAS Gateway 500 is not under warranty or an MA, then IBM refuses the service call. If the NAS Gateway 500 is covered under warranty, a Problem Maintenance Record (PMR) is created and the PMR number is returned to the Electronic Service Agent database on your system. This is reflected with an *OPEN* status in the failing NAS Gateway 500 PMR folder.
3. Electronic Service Agent is *not* intended as a replacement for the NAS Gateway 500 Warranty Package. All service calls should start with use of the standard Warranty Package. Electronic Service Agent is intended for use as an additional service tool.

Electronic Service Agent is an application program that monitors the NAS Gateway 500 for hardware errors, sends automatic service requests to IBM with no customer intervention, and collects machine inventory. Using the Electronic Service Agent, you can accomplish the following tasks:

- Automatic problem analysis
- Problem-definable threshold levels for error reporting
- Automatic service request transmission: service requests sent to IBM without manual assistance
- Automatic customer notification

- View hardware event logs
- Use secure Internet access or modem telephone line connection to IBM.
- VPD or machine inventory information can be sent to IBM
- Software product install and fix information will be sent to IBM

## How the Electronic Service Agent works

Figure 46 shows a typical NAS Gateway 500 Electronic Service Agent monitored network and how it relates to IBM.

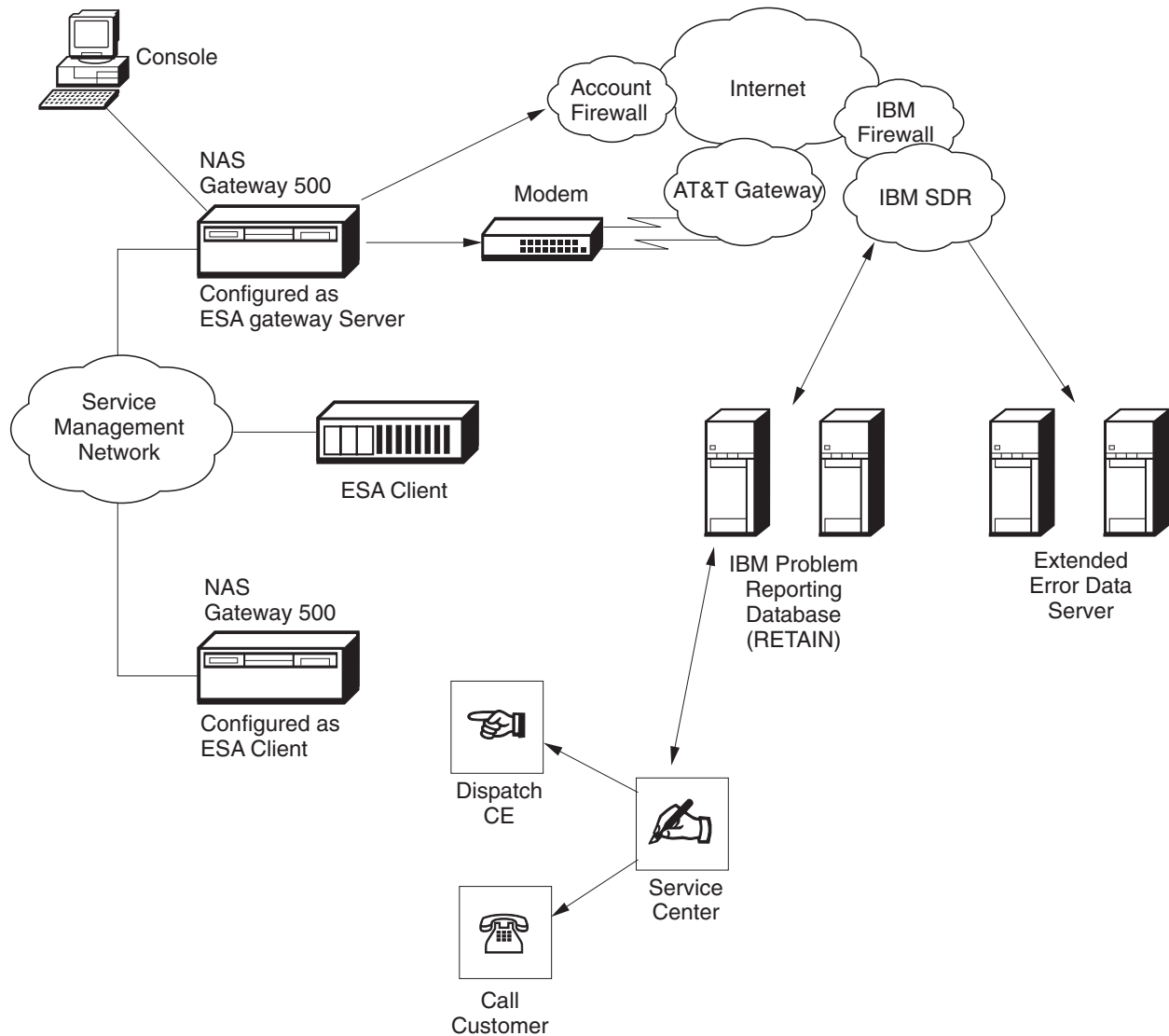


Figure 46. NAS Gateway 500 Electronic Service Agent monitored network and how it relates to IBM

The Electronic Service Agent is installed and defined on machines by using the Electronic Service Agent user interface. After machines are defined, they are enrolled with the IBM SDR. During the enrollment process, an electronic key is created that becomes part of the resident Electronic Service Agent program. This key is used each time that the Electronic Service Agent places a call for service.

The Electronic Service Agent is not designed to acquire any general information for which it has not been specifically programmed. Electronic Service Agent sends some data to IBM to assist with problem resolution. In some cases, this information can be used by IBM for other purposes. This information consists of the problem or error information itself, including Extended Error Data (EED), Vital Product Data (VPD), and Inventory data hardware or software.

## Inventory collection and vital product data (VPD)

An automatic service request does bring some inventory information with it. This is not the only inventory collection process within Electronic Service Agent. The Electronic Service Agent license text (confirmed at installation of Electronic Service Agent) on privacy and use of information states:

### Use of Information

“...the data gathered from these monitoring functions (“Your Information”) for purposes of problem determination, assisting you with performance and capacity planning, assisting IBM to enhance IBM products and services and notifying you of your system status and solutions we have available. Your Information excludes the collection and transmission of your financial, statistical and personnel data and your business plans.”

### **Preventing data from going to IBM:**

**Note:** All user data is fully encrypted during the transmission to IBM until used by an authorized party.

**Note:** In addition to error information, the only data that the Electronic Service Agent currently sends to IBM is VPD generated by the **lscfg** or **lsvpd** commands, or by the **invscout** program. Software commands **lsipp -hcq**, **instfix**, and **snap -g** can also be used. Run one of these commands to determine whether this information is sensitive.

If you think your data may be sensitive, you can review the actual data that is being sent to IBM using the Electronic Service Agent user interface or the command line interface. Review the data and determine whether you want Electronic Service Agent to send certain data. If you decide to prevent data from going to IBM, you can turn off the VPD gathering feature. This prevents transmission of VPD to IBM. You can prevent data from going to IBM with a modem (see “Using a modem”) or an e-mail server (see “Using an e-mail server”).

*Using a modem:* If you are using a modem, after enrolling, power off the modem and configure the Electronic Service Agent Notification process to notify your own help desk using e-mail, or have your help desk monitor the Electronic Service Agent in real time using the Electronic Service Agent Alerts function. If you choose this option, you must call IBM when the Electronic Service Agent detects an error; the Electronic Service Agent does not perform this step for you.

*Using an e-mail server:* If you have an active and accessible e-mail server, you can configure e-mail alerts to notify your own help desk, yourself or any other contact. Then, when the Electronic Service Agent detects an error, you can call IBM manually, instead of having the Electronic Service Agent do so.

**Note:** For information on setting up Electronic Service Agent to use e-mail notification, see “Adding an e-mail alert” on page 224. For information on the Electronic Service Agent Alerts function, refer to the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.

## Use of unsupported devices

The Electronic Service Agent can be configured to exclude devices not covered by IBM Warranty or maintenance agreement. When properly configured, unsupported devices (such as an unsupported tape drive attached to the external LVD SCSI port) are not reported to IBM. A range of devices can be defined with a single entry

using the resource names. Refer to the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide* for more information.

### Working with the NAS Gateway 500 and the central database

When you install the Electronic Service Agent program (svcagent.server) on the NAS Gateway 500, that server becomes the Electronic Service Agent gateway server by default. The active *hostname* of the machine becomes the default gateway machine name for Electronic Service Agent and is configured to be the reporting contact point for all communication interfaces. The communications interface to which the active hostname points to becomes the designated interface for all communications with Electronic Service Agent gateway server.

With the latest release of Electronic Service Agent, the hostname can be configured to a different communication hostname before Electronic Service Agent is started. The Electronic Service Agent database application registers socket 1199 as the Java RMI direct contact port on that named interface.

All configuration and setup data for monitored systems is maintained on the Electronic Service Agent gateway server and its central Java database. All monitored machines and Electronic Service Agent user interfaces are attached to and use that central database using Java to Java RMI communication over the default interface.

Figure 47 shows a typical Electronic Service Agent network.

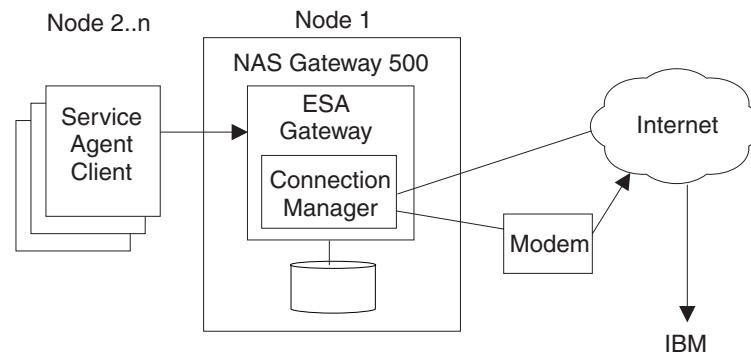


Figure 47. Typical NAS Gateway 500 Electronic Service Agent network

### Understanding modems and TCP/IP addressing

The Service Agent Connection Manager (SACM) can communicate with IBM using the Internet or modem. Because the SACM can handle input from a configured Electronic Service Agent gateway and client machine, a single Internet connection or modem is all that is needed to support a complex Electronic Service Agent configuration. Because redundancy can be achieved by using the secondary SACM as backup, a primary Internet connection to IBM could be backed up with a secondary dial setup.

**Note:** This is not done automatically. Manual intervention is required to switch between IP and modem connection to IBM.

If the existing TCP/IP allows connection to the Internet, the modem might not be needed. A modem can only be attached to serial port 2 (S2) on the NAS Gateway 500. This allows the Dialer to connect to the AT&T Gateway to access IBM service.

Appendix A, “Modem configurations,” on page 255 shows the proper basic modem setup for some IBM modems. The modem must be properly configured from the Electronic Service Agent user interface and Dialer menu before making calls.

### **Electronic Service Agent monitoring system**

Four major components or processes make up the Electronic Service Agent application:

1. Electronic Server System (ESS) process, running only on the gateway server
2. On Demand Server (ODS) process
3. SACM process
4. Basic or advanced ASCII interfaces

**Electronic Server System (ESS) process:** The ESS process runs only on the Electronic Service Agent gateway server, and handles all requests for data input and retrieval from the centralized database on the Electronic Service Agent gateway server. The ESS registers the RMI direct connect socket 1199 for the ODS or user interfaces applications to connect to the database.

**On Demand Server process:** ODS runs on all monitored machines including the Electronic Service Agent gateway, and handles all Electronic Service Agent monitoring and communication activities for that host. The ODS retrieves and sends data to the ESS process as necessary, or initiates a call to IBM. Any actual work or running of commands is done from the ODS. When the ODS initializes, it connects to the ESS using Java RMI. This communications link is maintained on a secondary available socket for the duration of the ESS. If communication is lost with the ESS, then the ODS automatically aborts and tries to establish the connection again.

Within the ODS, the Electronic Service Agent automatically monitors and reports major events to IBM, including:

- General health check
- Changes in the VPD, hardware and software
- Supported valid error events

Some of these events are reported to IBM directly using the Connection Manager configured communication method.

When a supported error event is detected, the Electronic Service Agent starts to prepare and send a request for service. It logs the event and reports the problem to the IBM problem management system for remote analysis and action (IBM RETAIN). If communications to the IBM RETAIN have been successful, a PMR number is returned and logged in the database with an Open status. The NAS Gateway 500 has Extended Error Data (EED) capabilities, and the EED information is sent to IBM TESTCASE server from the SDR. The associated file names are placed in the PMR for reference.

**Note:** You must define and enroll the machines that are to be monitored with the Electronic Service Agent to enable error detection. If you do not define and enroll the machines, the Electronic Service Agent does not capture any error information.

Additionally, the Electronic Service Agent can send e-mail notifications about all machine problem information (or limited problem information) to your help desk, yourself or other designated contacts. The e-mail notification functions must be

configured before they become active. See “Adding an e-mail alert” on page 224 for information on how to configure the e-mail notifications.

**Service Agent Connection Manager (SACM) process:** The Connection Manager was added to the Electronic Service Agent in order to satisfy the following user and IBM security requirements:

- Provide firewall support using either a proxy service or provide for traffic to pass through a Network Address Translation (NAT) device such as a Cisco PIX Firewall.
- Provide a single point of exit from a customer’s environment.
- Ensure Inter-Enterprise Security (IES) compliance.

The Service Agent Connection Manager is a standalone process that can be configured to communicate with IBM using an existing Internet connection or modem. This application is installed with the Electronic Service Agent AIX code on the Electronic Service Agent gateway.

**Basic and advanced ASCII user interfaces:** Basic and advanced ASCII interfaces allow you to set up and configure the Electronic Service Agent. The Basic User Interface allows a first-time user to configure the Electronic Service Agent system with as little user input as possible, using predefined defaults for a single-level network environment. The Advanced User Interface allows users to configure advanced functions and to customize the system as well as to configure it for complex systems and multilevel networks.

Navigation within the Electronic Service Agent is facilitated by keyboard data entry. Usually, a single key stroke is all that is required to navigate through the various menus. These key functions are defined within the help menus. Both advanced and basic user interfaces involve use of a logon password that defaults to password. IBM recommends that you change this password after your initial installation and store it in a safe place for security purposes.

## Service Agent security

This section discusses how security for the Electronic Service Agent works with the following areas:

- IBM Service Data Receiver using HTTPS
- Electronic Service Agent Connection Manager
- Global Dialer and Network
- Modem security

Access to the latest Electronic Service Agent security information resides on the following URL: [www.ibm.com/support/electronic](http://www.ibm.com/support/electronic).

- Select a **Country**
- Select **Electronic Service Agent**
- Under **Resources** expand General information
- Select the latest transmission security document for Internet and AT&T modem connection.

### Traversing secure boundaries

An Inter-Enterprise Service (IES) activity is the IT process of providing access to proprietary IT Resources. In providing that access the secure boundary of IT infrastructure must be traversed. Each communication path brings its own security requirements.

The Electronic Service Agent application was re-engineered to be IES-compliant for the NAS Gateway 500. It utilizes an HTTPS connection to the IBM SDR.

The Electronic Service Agent Connection Manager supports an https connection to the SDR. Because the Electronic Service Agent gateway implementations are coded in Java, and the Java Secure Socket Extension (JSSE) package is used, the Electronic Service Agent gateway needs to provide the SDR all the information it has about a given system during enrollment. This information can be pulled from the Node Info menu associated with the machine in question. This applies to both communication methods available for Electronic Service Agent: the Internet and the Dialer.

---

## Electronic Service Agent prerequisites

**Note:** The Electronic Service Agent is ready for installation on the NAS Gateway 500.

Before installing Electronic Service Agent, verify or complete the following steps:

1. Determine on which NAS Gateway 500, if clustered, Electronic Service Agent should be installed on and what method is used to connect to IBM. You can use an existing TCP/IP connection or a modem.
2. You must have root authority on the NAS Gateway 500 to enable and configure Electronic Service Agent.

**Note:** If you plan to install Electronic Service Agent clients during this configuration, you need root access to the client machines as well.

3. Ensure that your Electronic Service Agent gateway server has remote command capabilities (*rsh* *dsh*) or REXEC and FTP capabilities to all monitored clients (other nodes). If *kerberos* is on the Electronic Service Agent gateway server, ensure that there is a valid root ticket. In some cases, you might also need a valid ticket created for *svcagent* UID.
4. Ensure that IBM diagnostics are installed on every monitored machine. Error logging and error log analysis must be enabled.

**Note:** To determine if diagnostics are loaded, enter *diag* on the command line. Then, press the **Enter** key and select the *Task Selection* option of diagnostics. Scroll through the task list until you find and can select *Periodic Diagnostics*. Press **Enter** on the **Periodic Diagnostics Service Aid** main menu to get to the service aid list. The last entry shows the status of *Automatic Error Log Analysis* and allows you to switch states. Make sure that this entry is **ENABLED**.

5. Verify integrated diagnostics and extended error data:  
The Electronic Service Agent needs the *bos.diag.com* packages higher than 5.1.0.35.

**Note:** To verify your levels, enter the command **lslpp -l bos.diag.com**.

6. Verify your level of Java. Java is required on all monitored machines. Java versions supported are 1.1.8 to 1.4.0, with the later version displaying a much better performance characteristic. After Electronic Service Agent is installed, its path statement attempts to use the highest installed level of Java.

**Tip:** Enter the command *lslpp -l Java\**. This command displays the installed level of Java. If Java is not installed, you receive a message with that indication. If the tar format of Java was used to install it instead of the typical



installp version, the ODM entries might not exist and this command fails. In that case, run `java -version` to determine if it exists on the system. Ensure that the PATH statement for root allows for proper access to the level of Java that you want to use. Try the **which java** command .

7. If an existing Internet connection is to be used and no modem connection is needed, continue with step 12 on page 204. Complete the intervening steps only if you are using a modem connection for primary or secondary access to IBM.

#### **Modem communication steps**

8. Since your NAS Gateway 500 is your Electronic Service Agent gateway server, your modem must be attached to serial port 2 and a console to serial port 1. Make a record of which TTY device (for example, tty1) is mapped to serial port 2 (location: 01-S2-00). The **lsdev -Cc tty** command lists all TTY devices and their locations.

Verify the serial port TTY characteristics (such as tty1):

- tty interface is RS232
- baud rate is 9600 or higher
- login enable is disabled
- flow control is RTS

Use SMIT TTY to verify or change these settings.

**Note:** Do not change serial port 1 to **login disabled**. The service console access requires **login enable** be set to enabled.

9. The modem is used to register your NAS Gateway 500 and to call the IBM SDR. For security, only outbound calls are required by the Electronic Service Agent, so the auto-answer capability of the modem should be disabled. An asynchronous modem with a minimum communications speed of 9600 baud and error correction (in the United States) is required. Set the highest possible baud rate for your modem. Refer to local procedures in your country to see what the modem requirements are for the Electronic Service Agent.

Complete the setup instructions from Appendix A, "Modem configurations," on page 255 before using the Electronic Service Agent.

10. On your Electronic Service Agent gateway server, ensure that Point-to-Point Protocol (PPP) is installed and configured. PPP is only required if a modem is going to be used for error reporting to IBM. Following are the PPP Link configuration parameters with general minimum values. These values represent the minimum configuration required by the Electronic Service Agent.

If you plan to use PPP for anything else, these settings can be adjusted as needed. There should be an available 0.0.0.0 interface if properly configured. To prevent the setup server command from posting an error message, the 0.0.0.0 IP should be defined in **/etc/hosts** or DNS.

**Tip:** Enter the command **ps -ef | grep ppp**. Look for pppcontrol. If you find this, PPP is installed, configured, and running. Skip to the next step and check diagnostics.

If you cannot locate pppcontrol, enter **lsipp -l bos.net.ppp**. This command indicates whether the PPP file set is installed. If it is not installed, install the code from the AIX disk using SMIT. Return here and complete the following steps when PPP is installed:

- a. Enter `smit`.
- b. Select **Communications Applications and Services**.
- c. Select **PPP**.

- d. Select **Link Control Configuration**.
- e. Select **Change/Show a Link Configuration**.

If a configuration is displayed, then return to PPP and select **Start PPP**. If an error occurs, no link is configured. Follow these steps:

- a. Cancel out of **Change/Show** a link.
  - b. Select **Add a Link Configuration**.
  - c. Fill in the first nine parameters and accept the remaining defaults to build a single available client interface 0.0.0.0 IP:
    - PPP Subsystem name = PPP
    - max server connections(num) = 0
    - max client Connections(Num) = 1
    - max demand connections(Num) = 0
    - max IP interfaces(num) = 1
    - max async hdlc attachments(num) = 545
    - nru = 1500
    - async character map (Hex) = 454
    - transmit async character map (Hex) = 343
  - d. Press **Enter**.
  - e. Return to PPP and select **Start PPP**.
11. The modem should be connected to an analog telephone line and be operational. Check the physical connections to determine this. Remember the physical port that the modem is attached to does not equate to the assigned TTY port. Check TTY configuration to associate physical port to proper TTY.

**Continue here if no modem**

- 12. Prepare for e-mail alerts. The host that the e-mail is placed under must have e-mail service available either locally or through a network. To configure e-mail using the Electronic Service Agent configuration interface, see “Adding an e-mail alert” on page 224.
- 13. Obtain managed systems information. The Electronic Service Agent needs to know the host name, machine type, model, serial number, and processor-ID (should be auto filled) in order to monitor managed machines. This information is used during configuration of the Electronic Service Agent. The host name can be determined by typing the command **hostname** at the command line of the system being monitored. The serial number, model, and machine type must be obtained from the labels on the exterior of the machines. Do not use dashes or spaces when typing the serial number. Use the following table to record this information:

*Table 6. Managed systems information*

Host name	Machine type	Machine model	Serial number	Processor ID
	5198	001		

- 14. Predefine the svcagent user ID. The Electronic Service Agent defines the svcagent user ID to be used by the application. If the account has strict controls of machine UIDs, \$HOME directories, or other requirements, then the svcagent ID must be created before code is installed. The **mkgroup** is required to associate the UID and is needed for a clean uninstallation.

Enter the following commands:

```
mkgroup svcagent
mkuser pgrp='system' home='/u/svcagent' gecos='Service Agent Administration' svcagent
chuser shell='/usr/bin/ksh' login='false' rlogin='false' svcagent
```

---

## Installing the Electronic Service Agent

This section explains how to install the Electronic Service Agent on the NAS Gateway 500.

For your consideration: The Electronic Service Agent typically exports the client portion of the Electronic Service Agent program from the NAS Gateway 500 to monitored machines. This is done using FTP or remote commands, and requires root access to each client. If you have network security considerations and you do not want to FTP or rsh the code to what will be your monitored machines as root, see “Installing Electronic Service Agent client code manually” on page 208.

If you have custom requirements for your account user IDs, the Electronic Service Agent utilizes the predefined svcagent ID. See step 14 on page 204 for more information.

You can install the Electronic Service Agent on the NAS Gateway 500 using two different methods. The methods are:

1. Installing Electronic Service Agent from SMIT. See “Installing Electronic Service Agent from SMIT.”
2. Installing Electronic Service Agent from a command line. See “Installing Electronic Service Agent from a command line” on page 206.

**Note:** You can install this release of Electronic Service Agent over previous versions. **On an upgrade, you must install *svcagent.cm* last, after you have first installed the other modules.** Your machine list, communications files, and database remain the same. It is suggested that if you are migrating from Electronic Service Agent release 2.4 or older, utilize the following clean install procedure.

If you need to perform a clean install, first remove the old level of Electronic Service Agent. To simplify the configuration process after a clean install, first export the old Electronic Service Agent database; then, import it after the clean install is completed.

## Installing Electronic Service Agent from SMIT

1. Log on to the NAS Gateway 500 as *root*.
2. Type `cd /ESA` to access the Electronic Service Agent directory.
3. Enter `inutoc /ESA` (case-sensitive).
4. Enter `smit` (case-sensitive) to activate the SMIT.
5. Select **Software Installation and Maintenance**.
6. Select **Install and Update Software**.
7. Select **Install Software**.
8. Enter `/ESA` (case-sensitive) in the INPUT device/directory for software field.
9. Press **Enter**.
10. Enter **svcagent.\*** in the Software to install field.

**Note:** Using the asterisk (\*) selects all svcagent files. To install files separately, press **F4** and select the file or files you want to install.

11. Select **ACCEPT new license agreements?** If this field is set to **no**, Press **F4** and select **yes**.
12. Press **Enter**.
13. Press **Enter** to continue past the *ARE YOU SURE?* prompt.

**Note:** You should see SUCCESS in all the fields of the installation summary. (If you are using a hyperterminal session you may need to scroll up slightly) Sometimes the svcagent.cm may not load successfully. If the svcagent.cm package fails to apply successfully, rerun the **svcagent.\*** in the Software to install field. If the command fails again, continue by analyzing the installp faults. (See “Analyzing installp faults”).

Installation Summary				
Name	Level	Part	Event	Result
svcagent.cm		3.1.0.0 USR	APPLY	SUCCESS
svcagent.cm		3.1.0.0 ROOT	APPLY	SUCCESS
svcagent.client		3.1.0.0 USR	APPLY	SUCCESS
svcagent.client		3.1.0.0 ROOT	APPLY	SUCCESS
svcagent.help.en_US		3.1.0.0 USR	APPLY	SUCCESS
svcagent.msg.en_US		3.1.0.0 USR	APPLY	SUCCESS
svcagent.server		3.1.0.0 USR	APPLY	SUCCESS

Figure 48. Software install panel

14. Select **Cancel** after the Electronic Service Agent program installs.
15. Select **Exit** to exit the System Management Interface Tool.
16. You have successfully installed Electronic Service Agent for the NAS Gateway 500. Proceed to “Initial start of Electronic Service Agent processes” on page 210 to begin basic configuration.

## Installing Electronic Service Agent from a command line

1. Log on to the NAS Gateway 500 as *root*.
2. Type `cd /ESA` to access the Electronic Service Agent directory.
3. Enter `installp -acYXd .all` (case-sensitive).
4. Check the installation summary message result column to ensure that it indicates SUCCESS. If failure is indicated, continue with analyzing installp faults. (For additional information, see “Analyzing installp faults”).
5. You have successfully installed Electronic Service Agent for the NAS Gateway 500. See “Initial start of Electronic Service Agent processes” on page 210 to begin basic configuration.

## What to do if the Electronic Service Agent installation fails

If the Electronic Service Agent fails, you can:

- Analyze installp faults
- Review installp message flow

### Analyzing installp faults

You are in this analysis because the Electronic Service Agent installp process failed to post SUCCESS, and to help you determine the corrective action needed to

recover Electronic Service Agent. The installp process attempts to uninstall the Electronic Service Agent code if a fault occurs during the installation. To properly analyze the initial fault, find the first failing message. If you are not familiar with the installp flow, review the message flow topic.

The SMIT window automatically starts from the beginning of the installp process. If you are in a scrollable window using a bottom line command, scroll back to the **installp** command. If you are using a non-scrollable window and cannot see the initial failure but only the summary failure messages, run the listed cleanup command and reprocess the **installp** command using SMIT.

1. Review the installp messages for the first failing message posted.
2. If the problem has to do with prerequisites, insufficient core, or items that the system administrator can correct, fix the problem that has caused installp to fail.
3. If the problem is the making of the svcagent user ID, the system administrator can create the svcagent user ID manually and installp bypasses the step on the next installation. You need to create this ID on all of the monitored client machines also.
4. If a problem occurs within User or Root configurations routines that cannot be corrected by the system administrator, capture the messages and open a PMR against the Electronic Service Agent. If a problem is related to security or certain functions within the complex, record the concern in the PMR. In some cases, the application might not be able to properly exist on a customer complex. In all cases, do the cleanup steps and *do not* continue with the Electronic Service Agent installation process until the condition is resolved.
5. If the uninstalled function of the installp also failed, run the installp cleanup function as follows before reinstalling code again: enter **installp -C /ESA/svcagent.installp svcagent**. Optionally, you can replace svcagent with the individual module name if you are completing a selective manual clean install. Module names are:
  - svcagent.client
  - svcagent.help.en\_US
  - svcagent.server
  - svcagent.cm
6. Return to your selected installp process and reinstall Electronic Service Agent.

### Reviewing the installp message flow

To assist in familiarizing you with the events that occur during the installp process and to make reference for analysis easier, review the following flow. The SMIT window has available all the messages and information that was posted during the installp process. If being run from a command line, use a scrollable window to be able to view all messages. All of the numbered items have visual information to follow on all installations. The sub-bullets usually do not have any visual indicators unless a failure occurs during execution. There might be a clear message posted for the fault, or only the failing exit code. Within the flow, the failing exit codes are shown in parentheses ( ).

1. The first items shown are for pre-installation verification. This is where the prerequisites are verified. If a failure occurred here, install the prerequisites.
2. Next, the code is installed and you should see the copyright information.
3. Then, user configuration starts. A fault might occur here for these reasons:
  - Makes svcagent group(1), user(2), then builds svcagent profile(12). This prevents svcagent from being logged into as a user, but allows the Electronic Service Agent application code to run under an assigned svcagent ID.

- Sets up svcagent remote access to svcagent home directory(3).
4. Next, root configuration starts. A fault might occur here for these reasons:
    - Sets owner of /var svcagent files to svcagent(4), and execution level of /var.
    - Sets up /etc/rc.shutdown file for svcagent.
  5. Configuring the Electronic Service Agent gateway server, this is the first Java command to be executed. If Java is not properly set up, then this command can fail. If there is no /var/svcagent/properties file, then Java cannot be executed. This might be a path problem for Java or Java might not be installed. You might only see high CPU usage or time applied to /usr/svcagent/bin/ess script file.
  6. The Electronic Service Agent Property file is created on the Electronic Service Agent gateway server (message posted).
  7. The entries are made in inittab of the Electronic Service Agent gateway server for Electronic Server System and On Demand Server daemons.
  8. The database for the Electronic Service Agent gateway server is initialized and running (message posted).
  9. The last statement posted is the Installation Summary, which should be SUCCESS.

## Installing Electronic Service Agent client code

This section describes steps to install the client code on any machines managed by the Electronic Service Agent gateway machine. If there are no managed machines, skip this section.

### Installing Electronic Service Agent client code manually

The Electronic Service Agent typically installs the Electronic Service Agent client code on the monitored machines during configuration of the Electronic Service Agent gateway server. Electronic Service Agent uses FTP or remote commands to push its client code to machines that you want to monitor. The client code attempts to use the selected *Type of Install*, when you identify that machine using the *add machine* function. The automatic FTP process requires the Electronic Service Agent to use the root password or a root-authorized password.

If your network security configuration does not allow root FTP access to machines or RSH/DSH access, you can manually install the Electronic Service Agent client code using one of the following methods:

1. Install Service Agent Client using SMIT
2. Install Service Agent Client from command line

Before you select a method you must:

1. If you performed instructions outlined earlier in this section, ensure that the Electronic Service Agent program is installed on the machine that you intend to use as your Electronic Service Agent gateway server. (This should be done.)
2. Add the monitored machine or machines to the Electronic Service Agent gateway database. For the monitored machine On Demand Server to function, it must first be defined in the Electronic Server System database. To add a machine, see “Adding a machine” on page 222.
3. Select one of the following installation methods.
  - Electronic Service Agent client using SMIT
  - Electronic Service Agent client using CLI

## Installing Electronic Service Agent client code manually from SMIT

- Log on as *root* to the Electronic Service Agent client you want to monitor.
- Type `cd /ESA` to access the Electronic Service Agent directory.
- Enter `inutoc /ESA` (case-sensitive).
- Enter `smit` (case-sensitive) to activate the SMIT.
- Select **Software Installation and Maintenance**.
- Select **Install and Update Software**.
- Select **Install Software**.
- Enter `/ESA` (case-sensitive) in the **INPUT device/directory for software** field.
- Press **Enter**.
- Press **F4** to bring up a list of software to install.
- From the Software to install list, select **svcagent.client** and **svcagent.help.en\_US**.
- Press **Enter**.
- Press **Enter** to continue past the **ARE YOU SURE?** prompt.
- Select **Cancel** after the Electronic Service Agent client installs.
- Select **Exit** to exit out of the System Management Interface Tool.
- You have successfully installed Electronic Service Agent client.

## Installing Electronic Service Agent client from a command line

1. Log on to the NAS Gateway 500 as *root*.
2. Type `cd /ESA` to access the Electronic Service Agent directory.
3. Enter `installp -acYXd svcagent.client all` (case-sensitive).
4. Enter `installp -acYXd svcagent.help.en_US all` (case-sensitive).
5. You have successfully installed Electronic Service Agent client.

## Removing the Electronic Service Agent

This section describes how to remove the Electronic Service Agent from the NAS Gateway 500.

1. Log in as *root* on the NAS Gateway 500 machine that is the gateway server.
2. Type `smit`.
3. Select **Software Installation and Maintenance**.
4. Select **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. Enter `svcagent.*` in the SOFTWARE name field.
7. Set PREVIEW to **no** and press **Enter**.

You have deleted the Electronic Service Agent program from the gateway server.

## Uninstalling Electronic Service Agent on the monitored machine

### Removing Electronic Service Agent only using the Advanced Service Agent configuration

- Log in as *root* on the machine that is the Electronic Service Agent Gateway server.
- Bring up the Electronic Service Agent User Interface by issuing the following prompt sequence: **Smit** → **Problem Determination** → **Service Agent** → **Select**

**ServiceAgent User Interface** → **Select Advanced Text User Interface**. Then, enter the password. The default password is *password*.

- Expand the *Administration property*.
- Select **UnInstall**.
- Select **monitored machine** to uninstall.
- Select **UnInstall**.
- Complete the remaining prompts.

If you use the FTP protocol, the *Enter the User ID and Password* window appears. Type the password for root. If you can not use root and the root password, you can change the *User ID* field to a root-authorized user ID and use that ID's password.

To ensure the uninstall process is successful, monitor the window that appears with messages.

**Note:** This process leaves the monitored machine in the Electronic Service Agent database but removes the Electronic Service Agent program from the monitored machine.

---

## Initial start of Electronic Service Agent processes

The Electronic Service Agent daemons are no longer active when initial installation has completed, and must be initially activated.

Once the application has been successfully installed the various processes have to be manually configured and started. This only occurs after the initial or new installation, the upgrade process does not require this step because Electronic Service Agent is already running.

Determine what software has been installed and must be configured and started.

- Full installation of new Electronic Service Agent gateway.  
Complete "Step 1: Start Connection Manager" on page 211 and "Step 2: Start the Electronic Service Agent gateway" on page 211.
- Install only Electronic Service Agent client code.  
Complete "Step 3: Start the Electronic Service Agent client" on page 212. The host client should already be in the Electronic Service Agent database
- Install only Electronic Service Agent Connection Manager.  
Complete "Step 1: Start Connection Manager" on page 211 only.

After the required steps are completed, you should be able to continue the configuration of Electronic Service Agent information by selecting one of the Electronic Service Agent User Interfaces.

Use the following steps to get to the appropriate SMIT menu for Electronic Service Agent:

1. Type `smit` (case-sensitive) to activate the SMIT.
2. Select **Problem Determination**.
3. Select **Service Agent** (revision level).
4. Select the appropriate menu item to complete steps 1, 2 or 3 as described below.
5. Select **Cancel** when action is completed and to return to the Electronic Service Agent menu to complete other steps.



The status of Electronic Service Agent can be checked using Display Service Agent Status. This shows which processes are active on that host.

## Step 1: Start Connection Manager

**Note:** You need to verify the default configuration of SACM to the hostname and secure port 1198 if SACM is on the Electronic Service Agent gateway server (loopback may be used for efficiency).

- Select **Manage Service Agent Connection Manager**.
- Select **Configure Service Agent Connection Manager**.
  - Verify the default configuration of SACM to the hostname and secure port 1198 if the SACM is on the Electronic Service Agent gateway server.
  - The Listening hostname is blank on initial startup. If left blank, the SACM port 1198 listens on all network interfaces.
  - If account requires connection to listen to only one TCP/IP interface then insert the correct IP or hostname that points to the correct interface. This configures the SACM to the correct interface and port. You can also define the mode to a secure or unsecured assignment. If there is no need to go through a secure firewall to get to the SACM then you may want to use the unsecure assignment, because the access is faster. If you changed the Listening hostname, you need to change the CallController URL to SACM to match (This can be done later in the configuration.)
- Press **Enter**.
- Select **Cancel** twice when the action is completed. Then, return to the Electronic Service Agent Connection Manager menu to complete other required steps.
- Select **Start Connection Manager**.
- Press **Enter**.
- The SACM install is completed. For full install, continue with “Step 2: Start the Electronic Service Agent gateway.”

## Step 2: Start the Electronic Service Agent gateway

1. Select **Manage Service Agent Gateway**.
2. Select **Configure Service Agent Gateway** to define a different hostname, if desired, and to start ESA Gateway processes and add the inittab entries for database and ODS script.

**Note:** The default *hostname* of the Electronic Service Agent gateway server is the default configured host name.

You may also want to enter the machine type, model and serial data entry here. Otherwise, you are prompted for it later during Electronic Service Agent data entry and definitions. The machine type for the NAS Gateway 500 is 5198, model is 001, and the serial number is 7 characters. Do not use dashes or spaces when typing the serial number. Enter any alpha characters in these fields in UPPER CASE only. Auto discovery may have completed these fields if successful.

3. Press **Enter**.
4. Select **Cancel** when action is completed and to return to the Electronic Service Agent menu to complete other required steps.
5. Continue with the basic Electronic Service Agent configuration.

## Step 3: Start the Electronic Service Agent client

**Note:** This step is required if the Electronic Service Agent application did not install client code from Electronic Service Agent user interface.

1. Select **Manage Service Agent Client**.
  - Configure the client first; hostname is default, change if different hostname is in database. You have to enter the password to match the ESA gateway password.
  - The Primary (required), Secondary and Tertiary server hostname need to be defined.
  - You may to check the Machine Type-Model-Serial data if it was not properly filled with auto discovery process.
  - If hostname is already in the database the entry here is ignored.
  - The machine may also be placed under a Department heading by entering the desired department name that is defined in Electronic Service Agent gateway database.
2. Press **Enter**.
3. Select **Cancel** when action is completed and to return back to Electronic Service Agent menu to perform other steps.

Once the Electronic Service Agent gateway processes have been started, you should proceed to “Configuring the Electronic Service Agent.”

---

## Configuring the Electronic Service Agent

There are two interfaces available for configuring the Electronic Service Agent for NAS Gateway 500. You have the following ASCII versions available:

- Basic Electronic Service Agent configuration  
Used for initial, simple single network client machines that can address the Electronic Service Agent gateway server directly.
- Advanced Electronic Service Agent configuration  
Used for complex configurations and customizing of parameters. This is the primary User Interface for working with the Electronic Service Agent program. For example, the Advanced Electronic Service Agent configuration is used to perform a test call to IBM or test e-mail. Advanced Electronic Service Agent configuration is described in the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.

**Note:** The first time you configure the Electronic Service Agent on the NAS Gateway 500, you must go through the basic Electronic Service Agent configuration and complete the Electronic Service Agent gateway servers network and gateway required properties.

## Navigating the configuration panels

To navigate in an ASCII interface, you must use commands and respond to prompts to:

- Move forward
- Move backward
- Select and change specific options
- Save changes
- Access help

- Exit

Use the help text associated with the Welcome panel (for the basic ASCII interface) or the Main Menu panel (for the advanced ASCII interface) to find descriptions of how the navigation commands work.

### **Navigating in the basic ASCII interface**

The basic ASCII interface is designed to step you through the categories from beginning to end, one step at a time. It has the following categories:

- Network
- Gateway
- Dialer
- Machines
- Import/Export
- Registration
- Connection to IBM
- CallLog information

For example, if you were on the Network panel and wanted to go to the Machines panel, you would have to click **No** on the **Would you like to update** prompt for the Network, Gateway, and Dialer panels.

### **Navigating in the advanced ASCII interface**

The advanced ASCII interface is designed to let you choose options from a main menu. These options are available:

- Network
- CallLog
- Administration
- Alerts
- Filter Lists
- Manual Tools
- Test Tools

To move to any option, type the option on the command line and then press **Enter**. For example, to access Test Tools, type 7 on the command line and then press **Enter**.

After Electronic Service Agent has been configured, you can access advanced ASCII interface to configure such things as filters, alerts, e-mail alerts, pager alerts, and so on.

### **Menu key definitions**

All key inputs accept both uppercase and lowercase, when shown on the panel. Key definitions are as follows:

#### **[T]op Menu**

Pressing **T** moves you to the *top* of the menu selection list.

#### **[B]ack Menu**

Pressing **B** moves you to the *previous* menu selection list.

**[E]xit** Pressing **E** allows you to *exit* the program. You are prompted to confirm if you want to exit.

**[F <text >] - Find**

When in a text file or in a currently displayed list, entering **F**<*some text*> allows you to search for the *text* in that text file or list. The text search is not case sensitive. The *find* option is active with multiple window listings. Search starts from the current panel to the end of the file. After the first occurrence is located, entering **F** (alone) causes the display to locate the next occurrence. Line containing text is marked with ">" in the first column.

**[F[U] <text >] - Find**

Entering **FU**<*some text*> searches the text file or list for the entered text. The search starts on the currently displayed panel and searches to the beginning of the file. Entering additional **FU** continues the search upward.

**[N [#]] - Next panel**

Pressing **N** causes the next panel of information to be displayed. This option is active when the displayed text is greater than the display area of the program. Entering **N** <*some number*> jumps the display panel by the number entered.

**[P[#]] - Previous panel**

Entering **P** causes the previous panel of information to be displayed. Entering **P** <*some number*> jumps the display panel by the number entered.

**[#] - Select**

When this option is active, it allows you to make a selection from a menu.

**[#] - Modify**

When this option is active, it allows you to modify or update the displayed selection.

**[D#] - Delete**

When this option is active, it allows you to delete one of the entries displayed.

**[S] - Save**

After modifying or updating an entry, you *must* select the *Save* option to store the data into the Service Agent database. If the fields are changed but the **S** is not pressed, then when you exit a panel or interface a changed data reminder is posted, allowing you to return and either save, or exit and loose the entered data.

**Read Only and Mandatory**

If the fields that are shown have the letter *r* at the beginning, it means that such fields are read-only fields and you are not allowed to modify them. If the fields have an asterisk (\*) at the beginning, they are *mandatory* fields (that is the fields cannot be nulls or contain blanks). The \* is displayed when the field is blank.

## Accessing the basic configuration interface

1. Select **Select Service Agent User Interfaces**.
2. Select **Basic Text User Interface**.

**Note:** The graphics version is not supported by NAS Gateway 500.

3. Read and accept the license agreement during initial installation.

**Notes:**

- a. You are not asked to accept the license agreement if you selected **Yes** in step 11 on page 206.
  - b. The Electronic Service Agent basic window appears posting, Connecting to Server. This is where the user interface is establishing communications with the ESS on the Electronic Service Agent gateway server. If the password prompt does not appear within a minute or two, check Electronic Service Agent Status from the SMIT menu to verify that the server processes are running. If the password prompt does not appear on the Electronic Service Agent splash screen, the user interface is having problems connecting to the database process.
4. You are prompted for the password. The initial password is *password*. Type the password and press **Enter**. The Welcome panel is displayed.

**Note:** No characters are displayed when you type the password. The administrator should change this password to one that is unknown to anyone except authorized personnel to protect the Electronic Service Agent configuration setup from unauthorized modifications. Typing a wrong password causes an error message to be displayed indicating the password entered does not match the one expected. You have up to six chances to enter the password correctly. On the sixth mismatch, the logon quits and the user interface must be selected from SMIT again.

The password can be changed later by going to the administration folder and selecting the Electronic Service Agent access property later from the advanced interface. If the password has been changed, it carries the password to the new level of the Electronic Service Agent. To restore to the default password, you must complete a new or clean install of the Electronic Service Agent.

If Electronic Service Agent hangs, when you are expecting to get the password prompt, then the User Interface is not connecting to the ESS database process on the ESA gateway. Check that the `/var/svcagent/properties` file is pointing to the correct server. Check that the ESS process is running on the server with the `ps -ef | grep svca` command. Use `netstat -a | grep 1199` to see if the direct connect port has been properly registered. If this all appears to be correct, contact your IBM service representative.

5. Type **Y** on the Welcome panel, and then press **Enter** to continue.

```

IBM Electronic Service Agent for pSeries and RS/6000
version (R3.1.0.0) (Basic)
+-----+
| Welcome                                     |
+-----+----- screen 1 of 2 -----+
|
| Use the Service Agent Basic ASCII Interface to define monitored machines
| and configure a communications link to IBM so that Service Agent data can
| be sent to IBM for problem analysis.
|
| You need to update (or take IBM-supplied defaults) to the following prompts
| in the Service Agent interface:
|
| Network
| Gateway
| Dialer
| Machines
| Import/Export
| Registration
| Connection to IBM
|
|                                     [F <text>]-Find [H]elp
|                                     [N [#]]-NextScreen [E]xit
+-----+
| Would you like to continue? [Y/E] :

```

Figure 49. Welcome screen

- When you enter the ASCII interfaces the first time, you are prompted to complete certain required parameters and fields as shown in Table 7.

Table 7. Required parameters and fields for the ASCII interface

Field name	Input
Name of the customer that IBM support can contact	John or Jane Doe
E-mail address of the customer that IBM support can contact	doe@ company.com
Telephone number of the customer that IBM support can contact	1-123-456-7890
Address > Queue Country	162(USA) <sup>1</sup>
Gateway > Type	5198 <sup>2</sup>
Gateway > Serial Number	XXXXXXXX
Gateway > Model	001 <sup>2</sup>

**Note:** <sup>1</sup>Queue Country is selected from a list. Scroll using the **N** and **P** keys until you see your country. For information about navigating through the ASCII interface, see “Navigating the configuration panels” on page 212.

**Note:** <sup>2</sup>For NAS Gateway 500, the machine type is always 5198 and model is always 001. The serial number is located on the operator panel (front of the machine) just below the LCD. Do not include dash or spaces that may be shown in the serial number. For a description of the parameters, see “Network property” on page 227.

## Performing the basic Electronic Service Agent configuration

Complete the following steps to perform basic Electronic Service Agent configuration:

```

IBM Electronic Service Agent for pSeries and RS/6000
version (R3.1.0.0) (Basic)
+-----+
| Network                                     screen 1 of 1 |
+-----+
The Network Category allows you to update the following:
- Customer name IBM may contact
- IBM customer number
- Contact's phone number
- Contact's address

[H]elp
[E]xit

Would you like to update Network Data? [Y/N] :

```

Figure 50. Basic Electronic Service Agent Configuration wizard - Updating network data

1. Type Y at the *Would You Like to Update Network Data?* prompt.

```

IBM Electronic Service Agent for pSeries and RS/6000
version (R3.1.0.0) (Basic)
+-----+
| Network                                     screen 1 of 1 |
+-----+
1. Customer, IBM Support May Contact
2. Address
3. IBMCustomer Number
4. Telephone Number
5. Contact Context

[T]op Menu [B]ack Menu [H]elp
[E]xit

Options -> [#]-Select

User Input:

```

Figure 51. Basic Electronic Service Agent Configuration wizard - Entering updated network data

2. Enter the appropriate number or numbers to confirm the contact details, address, IBM customer number, context (general comments field), and telephone number. If you update any of the fields, remember to enter S at the user input prompt to save the changes before leaving the panel. For a description of the required parameters, see the “Network property” on page 227.
3. After all of the network parameters have been entered and verified, enter T to return to the Network main panel.

4. Enter N at the Would You Like Update Network Data prompt.
5. Enter Y at the Would You Like to Update Gateway Host Data prompt.
6. The **gateway** property should automatically be displayed with most of the information complete. (See Figure 52)

```

IBM Electronic Service Agent for pSeries and RS/6000
version (R3.1.0.0) (Basic)
+-----+
| ./Gateway Host -> IBM-5198001-0000000 |
+-----+----- screen 1 of 1 -----+
|
| 1. Name                : IBM-5198001-0000000
| 2. IPAddress           : 127.0.0.1
| 3. Processor ID        : 000000004C00
| 4. Type                 : 5198
| 5. Serial Number       : 1000001
| 6. Model                : 001
| 7. Manufacturer        :
| 8. Type Of Installation : ftp
| 9. Primary Server       : IBM-5198001-0000000
| 10. Secondary Server    : IBM-5198001-0000000
| 11. Tertiary Server     : IBM-5198001-0000000
|
| [T]op Menu  [B]ack Menu
|
| [H]elp
| [E]xit
+-----+
| Options -> [#]-Modify
+-----+
User Input:

```

Figure 52. Basic Electronic Service Agent Configuration wizard - Electronic Service Agent Gateway parameters

**Attention:** The *hostname* and *Processor ID* are retrieved automatically with the IP address of the Electronic Service Agent gateway server. The type, serial number, and model are required and must be accurate. If you update any of the fields, remember to enter S at the *User Input* prompt to save the changes before leaving the panel.

7. After all of the gateway parameters have been entered and verified, enter T to return to the gateway main panel.
8. Enter N at the *Would You Like to Update Gateway Data* prompt.
9. Enter Y at the *Would You Like to configure the CallController* prompt.
  - a. The item that needs to be verified and updated on this property template is the *Primary URL to Connection Manager* field.

**Note:** This defaults to **localhost**, which is appropriate if the SACM Listening Host Name was left blank. If the SACM host is a different host or if listening hostname is unique to a communications adapter, then the URL must be updated to reflect the correct hostname. If the hostname that the Connection Manager used during Initial Start of the Electronic Agent processes section (see “Step 1: Start Connection Manager” on page 211) was not blank, then set this field to match it. Also, if port was not default 1198, then correct the port number.

If Proxy is required to connect to Connection Manager, then you must update the Proxy fields. The proxy must be able to pass port 443 to allow proper connection.



10. After all of the CallController parameters have been entered and verified, enter **T** to return to the CallController main panel. If you update any of the fields, remember to enter **S** at the *User Input* prompt to save the changes before leaving the panel.
11. Enter **N** at the *Would You Like to configure the CallController?* prompt.
12. Enter **Y** at the *Would You Like to configure the ConnectionManager?* prompt.
13. The first item, *Connect to SDR using Dialer*, determines the method that Connection Manager uses to communicate with IBM.
  - a. If you are going to use an existing Internet or Intranet connection, this field must be set it to **false**.

*Connect to SDR using Dialer = false*

- b. If you are going to use a modem connection, this field must be set it to **true**.

*Connect to SDR using Dialer = true*

If you update this field, remember to enter **S** at the User Input prompt to save the changes before leaving the panel.

14. Enter **T** to return to the Connection Manager main panel.
15. Enter **N** at the *Would You Like to configure the Connection Manager* prompt.
16. If you choose **false** to the *Connect to SDR using Dialer* prompt, proceed to step 18 on page 220. If you choose **true**:
  - a. Enter **Y** at the *Would You Like to Update Dialer data* prompt.
  - b. Enter the appropriate number to set the Location field.
  - c. Select your country by number from the list. This brings up a city list. Select the closest city to your location. Additional fields are filled in automatically. Edit the primary telephone number to add any prefixes or special sequences required by your location (for example, 9 to get an outside line).
  - d. Enter the appropriate number to set the TTY # field. Enter the appropriate number (on the left) of the TTY for the serial port into which the modem is plugged (for example, 2 = TTY 1).

**Attention:** TTY 1 (Serial port 2) is used for the modem and TTY 0 (Serial port 1) is used for the boot console. Do NOT select the same TTY port number that the boot console is using. The terminal resets, and unpredictable results may occur.

**Note:** The modem has to be attached to the NAS Gateway 500 used as the Connection Manager server if communication with the IBM SDR is desired. If TTY port 1 is in use with a process that is logged on to it, Electronic Service Agent resets the port number and takes control when it accesses the port.

Enter the appropriate number to set the modem field. Select the modem that matches the one installed on your Electronic Service Agent gateway server (for example, 38 = IBM 7852-400). See Appendix A, "Modem configurations," on page 255 for further details on modem initialization and setup.

Opening and selecting a modem produces the values used in the *Reset String* and *Init String* fields. The modem strings are on an "AS IS" basis. They may need to be modified depending on the environment setup of your system. If the default modem does not match your attached modem,

you must verify the baud rate of your modem. You must select the highest baud rate that your modem uses. Selecting a baud rate greater than what your modem supports could cause the dial-out process to fail. The flag entry *Verify Baud Rate Before Dialing* is defaulted to *True*. This feature, starting with the baud rate you entered, attempts to automatically find the correct baud rate setting for the TTY. If necessary, modify the default reset and *init* strings to work with the modem.

- e. If you have a rotary or pulse phone system, enter the appropriate number to set the select the Dial Type field. Enter the appropriate number to set the dial type to *pulse* to match the type of telephone line used.
  - f. If you update any of the fields, remember to enter S at the User Input prompt to save the changes before leaving the panel.
  - g. If you update any of the fields, remember to enter S at the User Input prompt to save the changes before leaving the panel.
  - h. After all the Dialer parameters have been entered and verified, enter T to return to the Dialer main panel.
17. Enter N at the *Would You Like to Update Dialer Data* prompt.
18. If you are not adding a client to be monitored, enter N at the *Would You Like to Update Machine list?* prompt and proceed to step 19. If you are adding a client to be monitored, enter Y at the prompt and:
- a. Enter A to add a new client machine.

**Note:** If you need to delete the client machine you just added, enter D and the appropriate number (for example, D 1) to delete the client.

- b. Enter the appropriate number to set the new machine name, machine type, serial number, and model. This information represents the client machine that this Electronic Service Agent gateway server monitors. You can use either the IP address or the *hostname* (if you are using a name server) of the client as the machine name.
  - c. Enter S at the User Input prompt to save the changes before pushing the client code to the monitored machine.  
If you use FTP protocol, you are asked to provide the user ID and password of the client. Enter the user ID (use *root*) and password of the client machine when asked. If you cannot use root and the root password, you can change the User ID field to a root-authorized user ID and use the password for that ID.  
  
**Note:** After saving, if you want to modify any fields, you must delete the machine and input the information again.
  - d. If the Electronic Service Agent gateway cannot find the client code you are asked if you would like to copy the client code. Enter Y for yes.
  - e. Type `/ESA/svcagent.client` when you are asked for the location of the client code.
  - f. Press **Enter**.
  - g. After the client machine has been entered and verified, enter T to return to the Machine main panel and enter N at the *Would You Like to Update Machine?* prompt.
19. Enter N at the *Would You Like to use the Import/Export?* prompt.
20. If you do not want to enroll your Electronic Service Agent gateway server and client machine with IBM at this time, enter N at the *Would You Like to Enroll Machines* prompt and go on to the next step. If you are enrolling your Electronic Service Agent gateway, client, or both, enter Y at the prompt and:

- a. Select the machine that you want to enroll by entering R and the appropriate number.

**Note:** To enroll multiple machines, enter R, the appropriate numbers, each followed by a comma, and so on.

- b. Enter Y at the *Would You Like to Connect to IBM Now?* prompt. This action allows Electronic Service Agent to try to enroll your machines with IBM and takes you to the Call Log Properties panel. Check the description column to determine if your enrollment was successful or that it failed.
  - c. If your Electronic Service Agent gateway and client failed to enroll, your entitlement may not be activated. Contact service for help. If enrollment was successful, enter T to return to the Enrollment main panel.
  - d. Enter N at the *Would You Like to Enroll Machines* prompt.
21. Enter N at the *Would You Like to select the Connection option?* prompt.
  22. Enter N at the *Would You Like to Display the CallLog?* prompt.
  23. Enter Y to exit the Basic Service Agent Configuration.

You have completed the Basic Electronic Service Agent configuration.

If you did not enroll your client and want to add or customize a client, see the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.

## Configuration tasks

This section contains information on common tasks such as:

- “Adding a machine” on page 222
- “Installing the Electronic Service Agent code on a monitored machine only” on page 222
- “Specifying a machine’s physical location” on page 223
- “Specifying cluster details” on page 223
- “Defining resource filters” on page 223
- “Specifying thresholds” on page 224
- “Removing a machine” on page 224
- “Adding an e-mail alert” on page 224
- “Sending Vital Product Data (VPD) to IBM” on page 225
- “Setting up the Service Agent Connection Manager (SACM) to use the Internet” on page 225
- “Setting up Electronic Service Agent to use SACM” on page 225
- “Stopping and restarting the Electronic Service Agent process” on page 226

**Note:** See the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide* for additional tasks and information on folders, templates, template parameters and template fields.

Use the following steps to obtain the appropriate SMIT menu for Electronic Service Agent:

1. Enter `smi t` (case-sensitive) to activate the System Management Information Tool.
2. Select **Problem Determination**.
3. Select **Service Agent** (revision level).

4. Select **Advanced Basic Text User Interface**.
5. Type password as the initial password, and press **Enter**. The advanced panel is displayed:

```

                                IBM Electronic Service Agent for NAS Gateway 500
                                version  (R3.1.0.0) (Advanced)
-----current menu
-----panel 1 of 1

    1. Network
    2. CallLog
    3. Administration
    4. Alerts
    5. Filter Lists
    6. Manual Tools
    7. Test Tools

-----
Options -> [#] - Select
-----
User Input: _

```

Figure 53. Electronic Service Agent advanced panel

### Adding a machine

1. Select **Network**.
2. Select **A** (Add).
3. Select **Child**.
4. Select **Machine**.
5. Complete all the required fields for the selected machine (marked by an asterisk).
6. Select **FTP**, **DSH**, or **RSH** protocol option from the Type of Installation table.
7. Enter **S** to save the data.
8. If you use the FTP protocol, the Enter the User ID and Password window appears. Enter the password for root. If you can not use root and the root password, you can change the User Id field to a root-authorized user ID and use password of that ID.

### Installing the Electronic Service Agent code on a monitored machine only

To install the Electronic Service Agent code on a monitored machine only:

1. Select **Administration**.
2. Select **Un** (Uninstall).
3. Select **Install** and the appropriate client number.

**Note:** First select the host, scroll the range, hold the shift key and select ending host.

4. Enter **I** (Install) and the appropriate NAS Gateway 500 number.

If you use the FTP protocol, the Enter the User ID and Password window appears. Enter the password for root. If you cannot use root and the root password, you can change the user ID to a root-authorized user ID and use the password of that ID.

## Specifying a machine's physical location

Specifying the physical location of a machine helps service representatives provide prompt service to monitored machines.

1. Select **Network**.
2. If your client machine is under department, you must select **Department** first.
3. Enter A (Add).
4. Select **Form**.
5. Select **Location**.
6. Enter the correct data into the location template.
7. Enter **SS** to save the data.
8. Go back to the Network property folder of the machine you selected.
9. Enter I (Information).
10. Select **Location** to verify that the location template was completed.

## Specifying cluster details

1. Select **Administration**.
2. Select **Manage Cluster IDs**.
3. Enter A and select **machines to add Cluster I**.
4. Enter the cluster type, serial number and model.
5. Enter S (Save).

**Note:** If the selected system already has cluster information, a warning appears.

You can keep the existing information or overwrite it.

Adding the cluster information is a manual process, and this must be done for every individual system. In the case of an SP system, if the Cluster details are added to a CWS before the Add 9076 Nodes function is called, the function automatically adds the cluster details to every individual node. If the cluster details are defined, after the SP Nodes are added, it has to be done for every individual node (if they are part of the cluster). Cluster information is needed for proper routing of the problems on IBM retain.

## Defining resource filters

Resource filters allow you to specify certain devices so that they are not reported to IBM. This is particularly needed if the device is a non-IBM device not covered under warranty or a maintenance agreement. You can define resource filters for your network or for specific client machines. This example uses a specific client machine.

1. Select **Network**.
2. If your client machine is under department, you have to select **department** first.
3. Select **Machine**.
4. Enter A (Add).
5. Enter **Form**.
6. Enter Resource Filter.
7. Enter the name of the resource to filter or a range of resources.
8. Enter S (Save).

9. Verify your Resource Filter or filters by going back to the Network property folder of the machine you selected and enter **I** (Information).
10. Select **Resource Filter** to verify information.

### Specifying thresholds

Thresholds provide you with a way to prevent certain errors (for a network view or a monitored machine view) from being reported (by the Electronic Service Agent) to the IBM Service Agent Server (SAS). See the thresholds template in the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide* for information on how to determine errors (their id or number) that you can then use in defining thresholds.

1. Select **Network**.
2. If your client machine is under department, you have to select **department** first.
3. Select **Machine**.
4. Enter A (Add).
5. Select **Form**.
6. Select **Threshold**.
7. Enter the correct data into the Threshold template (error ID field).
8. Enter S (Save).
9. You can verify your threshold entry by going back to the Network property folder of the machine you selected and entering **I** (Information).
10. Select **Thresholds**.
11. Scroll until you locate the error that you just added.

### Removing a machine

1. Select **Network**.
2. Enter D (Delete), and then enter the appropriate number of the machine you want to remove.
3. Enter Y to complete the removal.

**Note:** This uninstalls the code on the machine and removes the machine from the Electronic Service Agent configuration.

### Adding an e-mail alert

1. Select **Network**.
2. Select a machine for which you want to create a E-mail alert folder. (E-mail alert is common for all the Electronic Service Agent clients on the same ESA gateway, irrespective of where we add the E-mail alert mechanism).
3. Select **Machine**.
4. Enter A (Add).
5. Select **Child**.
6. Select **EmailAlert**.
7. Change the default e-mail address to whom you want to send the e-mail. You can send an e-mail alert to multiple e-mail addresses by separating the e-mail addresses with a comma. For example, joe@host.companyname.com, carol@abcit.com, jill@companyname.com.
8. If the selected host has a different mail server, enter the name of that server as the value for e-mail server. The default name may be used if that mail server is the server performing e-mail serving.

9. Change the e-mail Wait Time in Minutes field to something quicker than 15 if you want to check the function or receive notification sooner than 15 minutes. You cannot use a value of 0.
10. Set to true the types of alerts of which you want to be notified. For more information and a description of the alert types, refer to the e-mail alert template in the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*.
11. Enter **S** (Save).

**Note:** Different e-mail alerts can be customized for particular users. For example, you may want employee A to be notified of CAUTIONS and employee B to be notified of INTERNAL ERRORS. Only one e-mail alert is normally needed for any events that might happen on any of the systems using this Electronic Service Agent gateway. Adding e-mail Alerts to individual nodes, does NOT provide details specific to those nodes.

### **Sending Vital Product Data (VPD) to IBM**

1. Select **Manual Tools**.
2. Select **VPD**.
3. Enter **S** (Send), and the appropriate number of the *monitored* machine for which you want to send manual VPD.
4. Send Manual VPD sends VPD to IBM at the next regularly scheduled time. Send Manual VPD Immediately commences to send VPD as soon as the option is clicked.

### **Setting up the Service Agent Connection Manager (SACM) to use the Internet**

1. Select **Network**.
2. Select the **Gateway host**.
3. Select **Connection Manager**.
4. Select **Connect to SDR using Dialer**.
5. Select **false** and press **Enter**.
6. Enter **S** to save.
7. Enter **T** (Top Menu) to return to user interface.

### **Setting up Electronic Service Agent to use SACM**

If you have a Connection manager making the connection to IBM, with either an existing Internet connection or a modem, the Electronic Service Agent gateway server may be configured to use the SACM to establish connection to IBM. Basically, you are deleting the Connection Manager and Dialer from this server and using an existing Connection manager.

1. Select **Network**.
2. Select the **Gateway host**.
3. Delete **Connection Manager**. (**D** and appropriate number).
4. Enter **Y** to delete **Connection Manager**.
5. Delete **Dialer**. (**D** and appropriate number).
6. Enter **Y** to delete **Dialer**.
7. Select **CallController**.
8. Enter the qualified hostname of the SACM server in the **Primary URL to ConnectionManager**. For example, *YourMaster.SACM.Server.Hostname:1198*.

9. Enter S (Save).
10. Enter T (Top Menu) to return to user interface.

### **Stopping and restarting the Electronic Service Agent process**

There may be times you want to stop or restart the Service Agent daemon process. There are multiple places where you have to interact with the Service Agent program to accomplish this:

- On the Gateway server ESS, ODS, and SACM (where the Electronic Service Agent database resides)
- On the monitored machines ODS only (clients that report to the Gateway server)

**Stopping the Electronic Service Agent daemons on the Electronic Service Agent gateway server:** Follow the steps below are used to stop the Electronic Service Agent daemon and remove inittab entries on the Electronic Service Agent gateway server:

1. Enter `smi t` (case-sensitive) from the command line. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent**.
4. Select **Manage Service Agent Gateway**.
5. Select **Stop Service Agent Processes**.
6. All of the Electronic Service Agent gateway server daemon processes are ended, and the inittab entries removed.

**Stopping the Service Agent daemon on the client machines:** Follow the steps below to stop the Electronic Service Agent program and remove inittab entry on the monitored or client machines:

1. Enter `smi t` (case-sensitive) from the command line of the client machine. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent**.
4. Select **Manage Service Agent Client**.
5. Select **Stop Service Agent process (ODS)**.
6. The client machine's Electronic Service Agent daemon processes are ended and inittab entry removed.

**Stopping the Service Agent Connection Manager:** Follow the steps below to stop just the Electronic Service Agent Connection Manager program and remove inittab entry on a standalone Connection Manager machine:

1. Enter `smi t` (case-sensitive) from the command line. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent**.
4. Select **Manage Service Agent Connection Manager**.
5. Select **Stop Connection Manager process**.
6. The Electronic Service Agent Connection Manager daemon process has ended and inittab entry was removed.

**Restarting the Electronic Service Agent daemons on the Electronic Service Agent gateway server:** After you have stopped the Electronic Service Agent daemons, you have to restart them on both the Electronic Service Agent gateway



server and the client machines. Follow the steps below to restart the Electronic Service Agent daemons on the Electronic Service Agent gateway server:

1. Enter `smi t` (case-sensitive) from the command line. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent**.
4. Select **Manage Service Agent Gateway**.
5. Select **Start Service Agent Processes**.

You have now created new inittab entries for the ESS, ODS, and SACM daemon processes that restart the Gateway server's Service Agent processes. If Connection Manager is not on this gateway then it is not started.

***Restarting the Electronic Service Agent daemons on the client machines:***

Follow the steps below to restart the Service Agent program on the Gateway server:

1. Enter `smi t` (case-sensitive) from the command line of the client machine. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent**.
4. Select **Manage Service Agent Client**.
5. Select **Start Service Agent processes (ODS)**.

You have now created a new inittab entry for the ODS daemon that restarts the client machine's Electronic Service Agent processes.

***Restarting the Electronic Service Agent Connection Manager:*** Follow the steps below to restart just the Electronic Service Agent Connection Manager program and add an inittab entry:

1. Enter `smi t` (case-sensitive) from the command line. If you are already in SMIT, go to the next step.
2. Select **Problem Determination**.
3. Select **Service Agent** (revision level).
4. Select **Manage Service Agent Connection Manager**.
5. Select **Start Connection Manager** process.

You have now created new inittab entry for the SACM daemon process that restarts the server's Electronic Service Agent Connection Manager process.

## Configuration property parameter details

This section describes the Configuration properties, parameters, and their fields.

### Network property

The Network property allows you to update the contact information for callback from the local IBM Support Center. The following fields are required:

- Name
- Telephone number
- E-mail address of the contact
- Country where the gateway server is located

After the data entry is complete, type **S** to save the data.

Table 8. Network properties

Parameter	Field	Description
<b>IBM Contact</b>	Name	IBM may contact for PMR discussions. (Required)
	Telephone number	Telephone number of contact. (Required)
	E-mail address	Internet e-mail address of contact. (Required)
<b>eService Information</b>	IBM Common Registration UserID	Your IBM Registration ID is your single point of access to IBM Web applications that use IBM Registration. You need just one IBM ID and one password to access any IBM Registration based application.  <a href="http://www.ibm.com/account">http://www.ibm.com/account</a>
<b>Address</b>	!Queue Country	Physical Country Location of the systems that PMRs will be open against. This will generally be the same country the contact Name of person resides in. However, if different the country where the Service Agent network is located should be used. (Required)
	Organization	Name of company. (Optional)
	Organizational Unit	Name of group or division. (Optional)
	Street	Street location where Electronic Service Agent Network is installed. (Optional)
	Locality	City, Town, or Village where Electronic Service Agent Network is installed. (Optional)
	State or Province	State or Province where Electronic Service Agent Network is installed. (Optional)
	Postal code	ZIP or postal code where Electronic Service Agent Network is installed. (Optional)
<b>Customer Number</b>	Customer Number	IBM customer number. (Optional)
<b>Standard Template Settings Parameter</b>		Default Template settings use across all monitored systems. Due to processing and system differences in a network all times indicated are approximate execution times.
	Err Lease - Days, Hours, Minutes, Seconds	This timer determines how long to keep and maintain host detected error entries generated by Electronic Service Agent.
<b>Telephone Number</b>	Number	Additional Telephone Number (Optional) Will become primary contact phone number if different from initial phone number.
<b>Contact Context</b>	Comment	Any comments that may help in communication between the company and IBM concerning support for the Electronic Service Agent monitored hosts.

**Notes:**

1. The country value selected is utilized to properly identify the systems and open Problem Management Reports (PMRs) based on country codes. The country selected must match that identified with the IBM customer number. If the country is incorrect, the PMR is rejected or sent to an incorrect queue.

2. The additional telephone number should be used for the IBM Support center contact point if the telephone number is different than the initial contact telephone number. If the first telephone number is for the central complex contact, but you want the IBM Support center to contact a different telephone number, enter the second number under the additional telephone number parameter.

### Gateway property

The Gateway property may be labeled with the name of the Electronic Gateway server instead of the name *Gateway*. This allows the Electronic Gateway server host to be identified by the name on this property. For example, if the Electronic Service Agent was installed on a NAS Gateway 500 called ABC, the second property button down from top is labeled *ABC*. The required fields for the node information parameter are:

- hostname
- processor ID
- type
- serial number
- model of the local machine

The hostname and Processor ID are not modifiable and are retrieved automatically along with the Electronic Gateway server's IP address. The type, serial number, and model are required input and must be accurate. If error is made in one of the locked fields after typing S, then Electronic Service Agent must be removed and reinstalled to correct the mistake. The auto discovery or "Get System Info" should aid in getting this data correctly, but still must be validated for accuracy.

After the data has been typed, type S to save the data.

*Table 9. Gateway properties*

Node information	Description
Name	Locked for host name of Electronic Service Agent gateway server. This field entry may be updated when an additional host is added.
IP address	Field is automatically filled in.
Processor ID	Locked, Uname -m number of local host. Field is automatically filled in; do not change.
Type	Required input — 4-digit number located on exterior of unit.
Serial number	Required — Serial number located on exterior of unit. Do NOT include dashes or spaces that may be shown in the serial number.
Model	Required — Model number of unit, three characteristics (001).
Manufacturer	Optional manufacturer name of unit (IBM).

Table 9. Gateway properties (continued)

Type of installation	<p>Determines the type of protocol used to distribute the client portion of the Electronic Service Agent program to selected monitored machines. The following protocols are available:</p> <p><b>FTP</b> This protocol is most frequently used. FTP prompts for a root authority ID and password. It uses the supplied password for transferring files using Java FTP protocol and running installation processes using the rexec.</p> <p><b>RSH</b> The RSH protocol must be configured to allow access for the svcagent user ID on the Electronic Service Agent gateway server to access the client system. One way to do this is to add to the .rhost file in the root directory the entry <code>&lt;gateway&gt; svcagent</code> where <code>&lt;gateway&gt;</code> is the hostname of the Electronic Service Agent gateway server or forwarding system to which the client is connecting.</p> <p><b>DSH</b> The DSH protocol allows the gateway to create nodes using the Distributed Shell system.</p>
Primary server (locked)	Used for internal functions within the Electronic Service Agent for the gateway server and subhost communication. Indicates primary host that subhosts report to. This field is locked on the gateway host and should not be modified.
Secondary server (locked)	Used for internal functions within the Electronic Service Agent for the gateway server and subhost communication. Indicates secondary host that subhosts report to. This field is locked on the Electronic Service Agent gateway host and should not be modified.
Tertiary server (locked)	Used for internal functions within the Electronic Service Agent for the gateway server and subhost communication. Indicates tertiary host that subhosts report to. This field is locked on the gateway host and should not be modified.

## Call Controller property

Table 10. Call Controller properties

Parameter	Description
Pending Timer In Minutes	When an event or problem is detected its status is set Pending. The value specified for the Pending Timer determines how many minutes to wait for additional events to be generated before taking action and attempting to make an external connection to the IBM SDR. For example if an error is detected at 1 PM, Electronic Service Agent will wait until 1:15 PM before taking action.
Check Open Status In Days	When a error event is set to an OPEN status, the value specified in this field determines how many days to wait before checking the status of the PMR on the IBM Problem Management side.
Health Check Timer In Days	The value specified in this field determines how often, (in days), Electronic Service Agent should call into the IBM SDR for a health check. It indicates that everything is OK including the communication. The countdown for this timer is reset whenever a good connection is made to the SDR
Max Retry Attempts	This value determines how many attempts to make a connection to the IBM SDR before giving up and setting the FAIL status of the events.
Current Retry Attempt	This value indicates the current connection attempt the CallController is on with the Connection Manager. When this count equals the Max Attempts count then FAIL status is set.
SACM Current Attempt	This value indicates the current connection attempt the Connection Manager to the IBM SDR.
Retry Timer in Minutes	This value determines how many minutes to wait before making the next connection attempt. If the Max Attempts is set to 3 and the Retry Timer is set to 5, then the CallController sleeps between each attempt for 300 seconds until the Max Attempts value is reached.
Connection Idle Timeout in Minutes	This value determines how long a connection can be idle (no activity) before a timeout condition is posted back to the CallController and breaking the connection to the Connection Manager. The default is 5 hours.
Primary URL to Connection Manager	This entry is the hostname or IP address and Port number of the SACM primary server. This value was defined by the SMIT Manage SACM configuration options. If <code>hostname:socket</code> was configured at that time, the default <code>localhost:1198</code> value should be corrected to correct <code>hostname:socket</code> .
Secondary URL to Connection Manager	This entry is the hostname or IP address and Port number of the SACM secondary server. It is normally blank.
Proxy IP to SACM	IP Address of the Proxy to connect to Electronic Service Agent Connection Manager. Leave blank if Proxy is <i>not</i> used.
Proxy Port to SACM	IP Address of the Proxy port number to access Electronic Service Agent Connection Manager. The default is 80.
Proxy Username	Username for SOCKS proxy in Strict mode. Leave blank if Proxy is <i>not</i> used.
Proxy Password	Password for SOCKS proxy in Strict mode. Leave blank if no Proxy is used.
Use Socks Proxy	When set to true, Call Controller utilizes a SOCKS Proxy to access SACM. The default is false.

## Connection Manager property

The Connection Manager template contains the entries and timers used to coordinate the call attempts to IBM SDR. There may be a backup SACM if high availability is required.

Table 11. Connection Manager properties

Parameter	Description
Connect to SDR using Dialer	When set to true, Electronic Service Agent uses the dialer (modem) to contact IBM Service Data Receiver. When set to false, Electronic Service Agent uses an existing Internet connection to contact IBM Service Data Receiver.
Minimum Gateways allowed to connect to ConnectionManager	This is the minimum number of Electronic Service Agent gateways. It should always be one (1).
Maximum Gateways allowed to connect to ConnectionManager	This is the maximum number of Electronic Service Agent gateways that can concurrently connect to SACM to utilize its call path.
Number of Gateways to be queued	This is the maximum number of Electronic Service Agent gateways that can be queued to Connection Manager if all available connections are busy.
Wait Timeout for Gateway in secs	This is the time out value in seconds. The default is two minutes. This should be set for less than the socket time out on a gateway.
Read Timeout for Gateway in secs	This is the maximum wait time for a read operation to be started. Default is two minutes.
The length of time the gateway connection can be alive in mins	This is the maximum time of Electronic Service Agent gateways can maintain any one connection. So, every five hours the connection must be released.
The URL for SDR	The complete secure URL definition for the IBM SDR.
The backup URL for SDR	The complete secure URL definition for the backup IBM SDR.
Timeout for connecting to SDR in secs	The maximum time allowed to make connection to the SDR. Default is two minutes
Read Timeout for SDR in secs	This is the maximum wait time for a read operation to be started. Default is two minutes
ChunkSize for data from Gateway to ConnectionManager in bytes	The data block size of transmitted information. The default is 2040.
ChunkSize for data from ConnectionManager to Sdr in bytes	The data block size of transmitted information. The default is 4080.
Delay between Chunks from ConnectionManager to Sdr in millisecs	This is the number of milliseconds to wait between data blocks. The default is 0.
The interval for the gateway monitor process on ConnectionManager in mins	How often the Electronic Service Agent gateway will check SACM process. The default is 2.

Table 11. Connection Manager properties (continued)

Parameter	Description
The size of the log for ConnectionManager in KB	Set the max size of SACM log in KiloBytes. The default is 2048.
Interval for the check for update to configuration files on ConnectionManager in mins	How often SACM should the ESS database for any changes to the Connection Manager configuration. The default is 30.
Dialer keep alive in secs	Interval for maintaining the dialer connection to prevent time outs. The default is 120.
Proxy IP to SDR	(leave empty if no proxy)
Proxy Port to SDR	The default port is 80.
Proxy Username	(leave empty if no user name)
Proxy Password	(leave empty if no password)
Use Socks Proxy	Set to true is you must use proxy to access IBM. The default is false.
Password for updating ConnectionManager configuration	password
Use Primary ConnectionManager URL	Set to true to utilize the Primary SACM URL. The default is true.
Use Backup ConnectionManager URL	Set to true to utilize the backup or secondary SACM URL. The default is false.

## Dialer property

The Dialer property allows you to define the modem parameters and account values for communication to the IBM SDR. In this entry, required fields are marked by the ! character, as in other screens within Electronic Service Agent. However, there is no verification of required fields for the modem parameters since a modem is not required for local setup of the rest of the Electronic Service Agent system. It is highly recommended to configure the modem from within the "Basic" interface at the time of installation.

See Appendix A, "Modem configurations," on page 255 for modem initialization and setup if you need additional information.

Table 12 describes the Dialer parameters.

Table 12. Dialer parameters

Parameter	Description
Location	The country or city the modem is calling to. By opening this table and selecting the country, then Detail. Finally select town telephone number closest to your location. Additional fields are automatically filled.

Table 12. Dialer parameters (continued)

Parameter	Description
! Primary Telephone Number	The telephone number the modem calls out to is populated according to the location selected. Change this telephone number only if needed. <b>Note:</b> Depending upon the local telephone exchange, this number may need to be modified to utilize your outgoing number and area code requirements.
Secondary Location	The second or backup country or city the modem is calling to.
! Secondary Telephone Number	The telephone number the modem uses to call in the event the primary telephone number fails.
! Account	The Service Agent network login account assigned by IBM. This can vary depending upon Location. Auto-filled does not change.
! User ID	The Service Agent network login user ID. This can vary depending upon Location. Auto-filled does not change.
! Password	The Service Agent network login password. This can vary depending upon Location. Auto-filled does not change.
! Primary Route - IP address SDR	The IP address for the SDR. This can vary depending upon Location.
Secondary Route - IP address SDR	The full hostname or IP address route for the SDR to use in the event the primary route fails.
Add DNS entries to /etc/resolv.conf	This set to true adds the primary and secondary nameservers to the <b>/etc/resolv.conf</b> file when initiating a dial, and removes them at the completion of the call. Setting to false prevents use of <b>resolv.conf</b> file.
! Primary DNS	The primary DNS IP used to access IBM SDR during dialing.
Secondary DNS	The secondary DNS IP used to access IBM SDR during dialing.
! TTY #	The available port number the modem is physically connected to.
Modem	The modem's reset and initialization string values are populated according to the modem selected. Change these values only if needed.  <b>Tip:</b> Type the first letter of the name to move quickly through the list.
Baud Rate	The maximum value the TTY modem will be set at for connection: 0 = 1,200 1 = 2,400 2 = 4,800 3 = 9,600 4 = 9,600 5 = 19,200 6 = 28,800 7 = 33,600 8 = 38,400 9 = 5,600
Reset String	The modem's initialization string values are populated according to the modem selected. Change these values only if needed.
Init String	The modem's reset string values are populated according to the modem selected. Change these values only if needed.
! Dial Type	Select the dial type of this modem (i.e. tone or pulse).



Table 12. Dialer parameters (continued)

Parameter	Description
Verify Baud Rate Before Dialing	Flag to verify baud rate selected works with the modem. If the baud rate fails, the program attempts to select the next best baud rate that works. The default is true. If the flag is set to false, no checking is done prior to running.
Max Retry Attempts	Maximum number of attempts the dialer tries to get a good connection to AT&T gateway. The default is 3.
Retry Timer In Seconds	Time in seconds the Dialer waits before attempting to retry. The default is 60.

## Enroll property

This property displays a list of all machines that have been defined. Enter **R** and the appropriate machine number allows you to register your machine with IBM.

Table 13. Register parameters

Fields	Descriptions
Register	After entering <b>R</b> and the appropriate machine number or numbers, you are prompted to either attempt to connect to the IBM Server Agent Server immediately, or wait until the timer for Pending process is triggered. You can select multiple machines to register by typing <b>R</b> , typing the appropriate number followed by a comma, then typing the next number, and so on.

## Connect property

The Connect property provides for immediate connection to the IBM Electronic Service Agent Server without waiting for any outstanding timer processes or the cancellation of the currently active connection. Upon connection, all entries in the queue for transmission to IBM are sent.

Table 14. Connect parameters

Parameters and fields	Description
Connect	Enter <b>1</b> and the program attempts connection immediately. The user is taken to the CallLog property panel where the real time status of the connection being made is displayed. See the CallLog property for details.
Disconnect	Enter <b>2</b> and the program cancels the current connection process and clears out all queues. All queued entries are set to a Failed status if appropriate. The CallLog property shows Canceled in the transmission description.

## CallLog property

The CallLog property displays a table of all calls made (or attempted) to IBM.

Table 15. CallLog parameters

Column	Description
Description	Displays real time connection updates as the connection is made. After the connection is ended, final Success or Fail results are logged here.

Table 15. CallLog parameters (continued)

Start time stamp	Time stamp of when the transmission started.
End time stamp	Time stamp of when the transmission ended.
Type	Type of call, LIC (padlock), PMR, and VPD Icon symbols.
Snd	This column is not used.
Rcy	This column is not used.
Try	Displays how many attempts it took to make the connection.
Status	Icon status of transmission. Green flag = OK.
TTY baud	If baud rate is established, posted connect speed or <non>.

## E-mail alert template

By adding an e-mail alert template, the Electronic Service Agent can send an e-mail message to contacts relating all or limited machine problem information. You can define as many e-mail contacts as you require, but an e-mail server must be active and accessible.

Table 16. E-mail alert template

Template	Description
E-mail Address	The e-mail address of the contact you want to alert.
E-mail Subject	The default subject line for messages.
E-mail Server	The hostname name of the mail server to be used.
E-mail Wait Time In Minutes	This field determines how long to wait in order to gather any additional notifications that can be generated. When the time specified is reached, all notifications gathered are combined into one e-mail notification and sent to the e-mail address.
Enabled	<b>Set the following Enabled and Urgent flags True/False accordingly.</b>
Cautions	An <i>Error Event</i> occurred that is considered a caution or informational entry.
Failed	A Electronic Service Agent <i>Error Event</i> transmission failed to open a PMR on the IBM Server Agent Server.
Held	An Electronic Service Agent <i>Error Event</i> entry was created and set to a Held status.
Pending	An Electronic Service Agent <i>Error Event</i> entry was created and set to a ending status.
Opened	An Electronic Service Agent <i>Error Event</i> transmission OPENED a PMR on the IBM Server Agent Server.
Closed	A Electronic Service Agent <i>Error Event</i> transmission CLOSED a PMR on the IBM Server Agent Server.
Internal Errors	An internal operating problem has occurred (e.g. inability to read a required file, or run a command, or anything that is detected with the operation of the Electronic Service Agent).
Licensing	There is a change in the licensing information for a machine. Either a machine has been licensed or it has expired.
PTF Updates	The machine has received notification that PTF Updates are available for download.
Electronic Service Agent Updates	The machine has received notification that the Electronic Service Agent Updates are available for download.

Table 16. E-mail alert template (continued)

<b>Template</b>	<b>Description</b>
Heart Beat	The machine failed a heart beat.
Performance	If an error is detected during PM/AIX data collection or transmission.
Test E-mails	This contact should receive any test e-mail's sent.
Extended Error Data	If fault occurs while collecting or transmitting extended error data.



---

## Chapter 32. Inventory Scout

Inventory Scout is a tool that surveys NAS Gateway 500 for hardware and software information. Inventory Scout can be used to collect the NAS Gateway 500's vital product data (VPD) and transmit this information, through the Electronic Service Agent (ESA) to IBM for matching with a Miscellaneous Equipment Specification (MES) upgrade.

When you run Inventory Scout it generates a data file that can be viewed. You can use this data file to see the current level of firmware loaded on the NAS Gateway 500 (for example, Adapters, System Software).

To run Inventory Scout from the command line:

1. Log in with root authority.
2. To run a microcode survey and create a text data file that can be read, enter **invscout** on the command line.

The resulting data file is created as `/var/adm/invscout/invscout.mrp`.

When you run the **invscout -v** command it generates a Vital Product Data (VPD) data file that can be viewed. You can use this VPD data file to see what is currently loaded on the NAS Gateway 500.

To run the Inventory Scout VPD tool from the command line:

1. Log in as root.
2. To run the VPD survey and create a data file that can be read viewed, enter **invscout -v** on the command line.

The resulting data file is created as `/var/adm/invscout/system_name.vup`.



---

## Chapter 33. Uninterruptible power supply

You might decide to purchase an external uninterruptible power supply (UPS) for your NAS Gateway 500. A UPS provides emergency backup power for a specified amount of time when local power fails. This power comes from batteries housed within the UPS. The actual amount of run time depends on the number and type of feature codes installed and the capacity of the batteries in the UPS.

The *Redundant or Interruptible Power for the IBM NAS Gateway 500 Technical Note* lists a set of supported UPS units.

---

### Configuring a UPS on the NAS Gateway 500

You must complete the product setup and installation instructions that came with your UPS before continuing. Your UPS batteries must be fully charged and the unit operational. To configure your UPS:

1. Install the UPS in the rack by following the installation instructions that came with your UPS.
2. Connect the NAS Gateway 500 power cords to the appropriate output receptacle or receptacles on the UPS.
3. Determine how you are going to monitor the NAS Gateway 500. Non-clustered systems can use either serial port or Ethernet signaling. Clustered systems must use Ethernet signalling.
  - a. If you are using serial port 3 (non-clustered systems only):
    - 1) Connect the NAS Gateway 500 to the UPS communication port using the communication cable that came with your UPS.
    - 2) Turn on the UPS.
    - 3) Install the necessary power management software (for example: LanSafe for LanSafe III) on the NAS Gateway 500.
    - 4) Configure the power management software on the NAS Gateway 500.
  - b. If you are using Ethernet signaling
    - 1) Connect an active Ethernet cable to the Ethernet port on the UPS.
    - 2) Turn on the UPS.
    - 3) Configure the Ethernet interface (for example: Assign a IP address) using the documentation that came with your UPS.
    - 4) Install the necessary power management software (for example: NetWatch) on the NAS Gateway 500.
    - 5) Configure the power management software on the NAS Gateway 500.
4. The power management software is now configured on the NAS Gateway 500. To ensure that the NAS Gateway 500 is protected from power failures, test it by simulating a power failure.
  - a. Disconnect the electrical power supply for the UPS. Do not disconnect the NAS Gateway 500 from the UPS.
  - b. The NAS Gateway 500 should remain operational.
  - c. Restore the main power to the UPS.

To test the ability of your UPS to signal a shutdown:

1. Disconnect the electrical power supply for the UPS.
2. Wait for the UPS to signal the NAS Gateway 500 to shutdown.

3. After the NAS Gateway 500 is powered off and OK is displayed on the operator panel. You can restore the main power to the UPS and power on the NAS Gateway 500.



---

## Chapter 34. System upgrades and configuration changes

This section describes the update procedures for the NAS Gateway 500. It is possible to upgrade the system hardware and software by ordering additional features such as, memory, adapters, clustering and so on. Firmware and software updates might also become available for download and installation.

---

### Adding new hardware

To add new hardware options to your NAS Gateway 500, use the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*. Be aware that hardware installation requires root access to the machine, and can require that the entire box to be powered off. After installation is complete, if software configuration is required, you will be referred back to this guide.

If you are adding hardware to a clustered node, you must not use the root command **cfgmgr**. This also means you must not use SMIT because SMIT uses the root default **cfgmgr**. You must always use the NAS command **/opt/nas/bin/cfgmgr** when adding hardware to a clustered node.

<b>Second Processor Book</b>	No additional configuration required.
<b>Additional Memory</b>	No additional configuration required.
<b>Ethernet PCI-X Adapter</b>	Set IP address or addresses.
<b>Fibre Channel HBA</b>	Configure SAN storage first, then no additional configuration required.
<b>OS Mirroring</b>	Configured during installation of FC 1001. Refer to the <i>IBM TotalStorage NAS Gateway 500 Hardware Installation Guide</i> .
<b>Clustering</b>	Configuration required.
<b>Remote Mirroring</b>	Configuration required.

---

### Adding a network adapter

If an Ethernet network adapter is added, the network administrator must be notified so that the client IP addresses can be assigned to the new adapter card. In addition, the operating system configuration of the network adapter will need to be completed based on the information provided by the network administrator. Also check to ensure that any client or server access is maintained.

To set IP addresses of the Ethernet interfaces, see Chapter 26, “Managing networking,” on page 149. For advanced configuration of Ethernet interface properties, such as media speed negotiation or jumbo frames, refer to the *IBM TotalStorage NAS Gateway 500 Advanced Configuration and Problem Determination Guide*

---

### Adding a Fibre Channel HBA

If a Fibre Channel HBA is added, the SAN administrator must be notified so that the adapter definitions on the SAN storage and the Fibre Channel zones on the SAN switches can be updated with the WWPN of the new adapter. See “Displaying additional device-specific information” on page 121.

**Note:** Before attaching any NAS Gateway 500 Fibre Channel HBA to SAN storage, that storage must be already configured. Otherwise, the NAS Gateway 500 will take an exceptionally long time to resolve the SAN pathways, and may hang for hours with a “581” displayed on the operator panel.

---

## Adding Remote Mirroring

For a field upgrade from a single site to a dual site with Remote Mirroring, contact IBM or check the IBM support Web-site for the most up-to-date procedures and instructions. The Web-site is [www.ibm.com/servers/storage/support](http://www.ibm.com/servers/storage/support).

---

## Adding clustering

**Note:** For the most up-to-date procedures and instructions, contact IBM or check the IBM support Web site. The Web site is [www.ibm.com/servers/storage/support](http://www.ibm.com/servers/storage/support).

This section provides information on field upgrading from a single node gateway to a dual node cluster

### Before you begin

1. Ensure that the new NAS Gateway 500 system (joining node) to be upgraded has a fresh factory image with a default factory password of *password*, integrated port #2 is set to an IP of 192.168.244.1.  
  
**Note:** If you have two previously configured single nodes, then one of the nodes must be re-imaged using the NAS Gateway 500 Recovery CDs before you start the upgrade. Both nodes must have integrated Ethernet port #2 set to the default IP address of 192.168.244.1.
2. Review the NAS Gateway 500 Planning Guide for information on planning for clustering. Fill out the cluster planning worksheet with the required or applicable information.
3. Verify if Tivoli applications (such as Tivoli Storage Manager Client, TSM Storage Agent, Tivoli Storage Resource Manager Agent, and Tivoli Storage Area Network Manager Agent) have been configured and enabled on the existing node. If they have, disable the service from starting on boot. This can be accomplished through SMIT or WebSM.
4. Ensure that both nodes (the existing and joining nodes) are properly cabled and connected to the backend storage device (such as FAStT or ESS). Ensure that you have the correct driver installed for the backend storage (SDD for ESS or SAN Volume Controller) on both nodes.
5. If the backend storage is different from what was previously connected to the existing node, make sure the operating system is able to discover the new configuration before the upgrade. This can be accomplished by either rebooting the node or issuing the **cfgmgr** command at a command line to add and configure new devices.
6. Connect two NAS Gateway 500 nodes (the existing and joining nodes) using a NULL modem cable between serial ports #3, and an Ethernet crossover cable between integrated Ethernet ports #2.
7. Ensure both nodes are powered on and have completed all power-on self testing.

## Upgrading the system

1. Export volumes from the existing node. If volumes had been previously defined on the existing node which will now be part of a cluster, and those volumes are to be restored after the upgrade, then the volumes must be exported now. Once cluster configuration is complete they can then be imported to the dual-node system. To export volumes from the existing node system:
  - a. Log in as root user to the existing single-node NAS Gateway 500.
  - b. Run the `/opt/nas/bin/lspvol` command and record the information on each physical volume identifier (PVID) and its corresponding volume.
  - c. Record and remove all NFS exports and CIFS shares (this can be done through SMIT or WebSM).
  - d. Run the `/opt/nas/bin/expvol <volume to be exported>` command on all volumes.
2. Run WebSM Initial Configuration Wizard on the joining node:
  - a. **Note:** Skip this step if you already have the remote client installed on a graphics-capable machine. There is no need to download and install this client again.

Point your browser to the IP address of the joining node. Select **Language→Continue→Download** (WebSM setup.exe) to install WebSM client, if necessary. Execute WebSM setup.exe to create a WebSM client icon on your desktop.
  - b. Click on WebSM client icon, fill in Host Name (is the IP address of the node), and log on as root user to the joining node. The Welcome screen appears on the upper left corner.
  - c. Click the Initial Configuration Wizard, and select your purchased features from the Feature management screen:
    - Clustering feature (a single-site, dual-node cluster is configured if this feature is selected without Remote Mirroring)
    - Remote Mirroring (a dual-site Geographic Cluster is configured if this feature is selected)
    - CIFS feature (a CIFS server is configured if this feature is selected)
  - d. Fill in the rest of the screens as appropriate. Any NAS Administrators and file access users must be redefined (either during or after WebSM initial configuration), so that they exist on both nodes of the cluster.
  - e. Create additional new volumes as needed. If you do not need to create new volumes, continue past the Volume Management screens and click **Finish** to exit the wizard.
3. Import the volumes that were exported from the existing node to the newly configured dual-node cluster:
  - a. From the Web-based System Manager window, select **NAS Management→NAS System→Volumes→Overview and Tasks→Import a NAS Volume**.
  - b. Select the new group from the pull-down list. This new group may be the original node where this volume was exported or the new joining node. Complete the New Volume Name, and select Disk Containing Volume from the pull-down hdisk list whose PVID corresponds to one of the PVIDs on which the volume resides (using the information recorded in step 1b). Click **OK**. Repeat for all volumes to be imported.
  - c. After importing the NAS volumes, recreate the NFS exports and CIFS shares, using the information recorded in step 1c). Click **Start local CIFS server operations** to start the CIFS server if necessary. From Web-based

System Manager window, select **NAS Management**→**NAS System**→**File Serving**→**CIFS**→**Overview and Tasks**→**Create a new file system share**.

4. **Note:** This step is necessary only if Tivoli products were configured and running on the existing single-node NAS Gateway 500 system, and were disabled when you completed step 3 on page 244.

Reconfigure and start all Tivoli applications. At this point, the NAS Gateway 500 is set up as a clustered configuration. In order to configure the Tivoli applications on both nodes, you must reconfigure the following:

- a. Start the previously stopped processes.
- b. Enable the previously disabled applications.
- c. Reconfiguration can occur from either node, but it is preferred to reconfigure from the existing single node; this node has the current settings for the Tivoli applications already configured.
- d. Once reconfiguration is complete and saved, the configuration information is propagated to the other node in the cluster. The starting of applications and boot settings will be set on both nodes now that the environment is a clustered environment.

---

## Software system upgrades

The NAS Gateway 500 software updates will be provided by way of AIX Maintenance Releases, Program Temporary fixes (PTFs), NAS System Software Updates and Firmware Updates. Details for supported updates and fixes for the NAS Gateway 500 will be posted regularly on the NAS Gateway 500 support Web site.

Downloading the software updates and update instructions from the Web is preferred.

Always check the NAS Gateway 500 Support Web site for the latest updates and instructions. The Web address is:

<http://www.ibm.com/servers/storage/support/download.html>

## Installation and Packaging of Updates

NAS Gateway 500 updates are supported in the following installation formats:

- RPM Package Manager (RPM)
- Install Shield MutliPlatform (ISMP)
- Installp

The Web-based System Manager, SMIT, or CLI can be use to install and uninstall these types of packages. The **installp** command is a root user CLI command that allow the installation and removal of software packages within the installp format. The command **geninstall** is a root user command that is a generic installer, capable of recognizing and installing packages within RPM, ISMP, or the installp format.

When a filesset update is applied to the system, the update is installed and the current version of that software, at the time of the installation, is saved in a special save directory on the disk so that the update can be removed and preload software be can returned to the previous version if desired. This flexibility allow updates to be uninstalled to the previous version seamlessly.

## Types of Update packages

### System Software Maintenance Release

System Software Maintenance Release/Level consists of one fileset update for each fileset that has changed since the base level of the release of NAS Gateway 500. Each of these fileset updates are cumulative, containing all fixes for that fileset since the official Release was introduced, and supersedes all previous updates for the same fileset. A Recommended Maintenance Release, is a subset of fileset fixes created for a group of APARs since the most recent Maintenance Release.

Maintenance Release updates are nondestructive and usually require a reboot of the system. Supported Maintenance Release will be listed using the support Web site.

### PTF

A PTF is a code fix that can be shipped to customers to fix specific problems (APARs) on a system. A single PTF often ships multiple files and often fixes multiple APARs. PTFs are nondestructive; however, based on the software component affected by the fileset updated, a reboot of the system may be required (note: most Kernel fileset updates will require a reboot).

Recommended PTFs will be available to the Customer via Internet download.

### NAS System Software Update /EC Release

The NAS Software Update is a mechanism to update the NAS system software preload in the field and Manufacturing with the latest fixes. The Update will contain the latest software updates since the latest NAS software preload build or software update. Updates are nondestructive; however, based on the software component affected by the fileset(s) updated, a reboot of the system may be required.

### Firmware Updates

Firmware initializes, or sets up, the hardware configuration so that your system will boot up and operate correctly; it provides the interface to the system software to control the hardware. Adapter microcode is the operating code of the adapter; it initializes the adapter when power is applied and it controls many of the on going operations executed by the adapter. The NAS Gateway 500 was developed and tested at a specified firmware level, in which various adapters and software components are integrated into one solution. Firmware updates will be posted on the NAS Gateway 500 support Web site.

Firmware updates will require a reboot of the system and will be nondestructive. See “System firmware updates” on page 248 for more information.

## Software update practices

Depending on the type, software updates can be limited to only a single component and can range to multiple filesets. Updates should not affect the configuration of the NAS Gateway 500. However, a reboot might be required if the update is Kernel level based update.

---

## System firmware updates

This section provides information and instructions for updating the system firmware. You may need to perform these steps if you are installing an option or if your support representative has instructed you to update your firmware.

If you cannot download from the Web, do the following:

- If the system cannot be powered on, but the service processor menus are available, see “Using the service processor menu method” on page 249.
- If the service processor programming has been corrupted, the service processor will automatically enter recovery mode when power is applied to the system.

To check the level of firmware that is currently on the system, see “Determining the level of firmware on the system.”

## General information on system firmware updates

All the system firmware types that can be reprogrammed are updated at the same time. They are:

- System-power-control network programming
- Service processor programming
- IPL programming
- Run-time abstraction services

Retain and store the latest firmware diskettes each time the firmware gets updated in the event that the firmware becomes corrupted and must be reloaded.

## Determining the level of firmware on the system

The firmware level can be checked using the CLI or in the service processor main menu. To check the firmware level, enter the **# lscfg -vp | grep -p Platform** command. This command will produce a system configuration report similar to the following:

```
Platform Firmware:
ROM Level.(alterable).....RR031014
Version.....RS6K
System Info Specific.(YL)...U0.1-P1/Y1
Physical Location: U0.1-P1/Y1
```

The firmware level is denoted by XXYYMMDD, where XX = model designation, YY = year, MM = month, and DD = day of the release.

The second line of the service processor main menu title (for example, Version: 3R031014), shows the currently installed firmware level. If the firmware level is correct and not update is needed, installation is complete.

## Updating the firmware

The system, service processor (SP), and the System Power Control Network (SPCN) firmware are combined into a single file. This allows all the firmware to be updated together and assures that they are compatible. Once the system and service processor firmware has been updated, the NAS Gateway 500 will reboot. The SPCN update will continue to run in the background.

**Attention:** Ensure that the system is not running any user applications when you begin the update process. Do not power off the system at any time before the update process completes.

Checksums should be used to verify that files have not been corrupted or altered during transmission. At the command line, enter: `sum XXYMMDD.img`. The output will look similar to the following:

```
12129 4837 XXYMMDD.img
```

In this example, the checksum is 12129.

Updating firmware must be initiated directly from the service processor menus or from the command line.

## Using the service processor menu method

Service processor menus allow updating from diskettes only. You must have privileged user authority (if service processor passwords have been set) on the NAS Gateway 500 to update its firmware, and you must have console attached to serial port 1.

**Note:** All firmware (system, service processor and SPCN) will be updated when using this method.

1. Shutdown the server from a tty terminal window connection.
2. When the operator panel on the server says OK, press **Enter** to bring up the service processor menu.
3. Select **Service Processor Setup Menu**. Press **Enter**.
4. Select **Reprogram Flash EPROM Menu**. Press **Enter**.
5. Enter **y** to continue. Press **Enter**.
6. Follow the on-screen update steps as they are presented.
7. The Rebooting Service Processor message appears on the screen. The NAS Gateway 500 will reboot. This can take up to thirty minutes, depending on the configuration of the target server. Because the update occurs during this shutdown/reboot sequence, it is important to protect the server from interruptions.
8. Begin watching the operator panel. Possible message codes are described in "Recovery mode."
9. When the panel indicates OK, press **Enter**. The service processor menu appears on the screen. The second line of the title, Version: XXYMMDD, should match the firmware level you just installed.

The firmware update is complete.

### Recovery mode

Code	Action
A1FD 0000	System firmware has been corrupted and must be reflashed.
A1FD 0001	Insert update diskette 1.
A1FD 0002	Insert update diskette 2.
A1FD 0003	Insert update diskette 3.
A1FD 000 <i>n</i>	Insert update diskette <i>n</i> .

**Notes:**

1. If the wrong diskette is inserted at any time, or if the diskette is left in the drive after it has been read, B1FD 001F is displayed, indicating that the wrong diskette is in the drive.
2. If B1FD 001A is displayed at any time during the process, the service processor must be reset by activating the pinhole reset switch on the operator panel.

## Using the CLI method

You must have root authority on the NAS Gateway 500 to update its firmware. This method allows updating from files already loaded onto the NAS Gateway 500. For example, if the file is located in the /tmp/fwupdate/ subdirectory, enter the following commands:

```
cd /usr/lpp/diagnostics/bin  
./update_flash -f /tmp/fwupdate/3R030718.img
```

**Note:** Do not overlook the periods (.) in the above command.

You will be asked for confirmation to proceed with the firmware update and the required reboot. If you confirm, the NAS Gateway 500 automatically performs the update and reboots. The checkpoints 99FF and 99FD alternately appear while the update is in progress. This can take up to thirty minutes, depending on the configuration of the system. Because the update occurs during this shutdown/reboot sequence, it is important to protect the NAS Gateway 500 from interruptions.

To verify that the update was successful, the firmware level can be checked as described in “Determining the level of firmware on the system” on page 248.

## Archiving the update files

In the event that it becomes necessary to restore the server to a certain firmware level, you should identify and archive the materials for each update you install. If the download process produced diskettes, label and store them in a safe place. If the download process produced files, archive and identify the files for convenient retrieval.



---

## Chapter 35. Miscellaneous administration tasks

This section describes miscellaneous administration and integration tasks for the NAS Gateway 500.

---

### How to change SNMP V3 for single node

Although SNMP version 1 is the default on the NAS Gateway 500, you can, with root authority, optionally change a single-node gateway configuration to SNMP version 3.

**Note:** SNMP version 3 is not a supported feature on any clustered configuration.

Use these commands to modify the version of SNMP:

To change to the snmpdv1 agent, enter: `/usr/sbin/snmpv3_ssw_1`. This the default.

To change to the encrypted version of the snmpv3 agent, enter:  
`/usr/sbin/snmpv3_ssw -e`

To change to the non-encrypted version of the snmpv3 agent, enter:  
`/usr/sbin/snmpv3_ssw -n`

**Note:** This process requires root user authority.



---

## Part 6. Appendixes



---

## Appendix A. Modem configurations

**Attention:** This appendix applies only to modems attached to serial port S2 located on the CEC backplane (location U0.1-P1).

Verify the TTY characteristics of serial port S2.

- tty interface is RS232
- baud rate is 9600 or higher
- login enable is disabled
- flow control is RTS

Use the **smit tty** command to verify or change these settings.

**Note:** Do not change serial port 1 to **login disabled**. The service console access requires **login enable** be set to enabled.

The Electronic Service Agent is designed to place little demand on an attached modem, thereby increasing the setup and connection success rates.

**Note:** This information replaces Appendix B, in the *IBM TotalStorage NAS Gateway 500 Service Guide*.

---

### Modem setup

This section describes how to configure the IBM modems recommended for use with the Electronic Service Agent.

The recommended modems are:

- 7852 Model 400
- 7857-017 or 7858-336

**Note:** You can use a non-recommended modem. The Electronic Service Agent configuration has an extensive selection of modems from which you can choose.

Use the following steps to select a configuration file:

1. Is your modem an IBM 7852-400? If so, see “Configuring the 7852-400 Modem” on page 256 to set the dual in-line package (DIP) switches on the modem.

**Note:** The IBM 7852-400 modem has DIP switches on the right side of the unit. See “IBM 7852-400 DIP switch settings” on page 257 for the correct switch settings.

2. Is your modem an IBM 7857-017? If so, see “Configuring the 7857-017 or 7858-336 Modem” on page 256.

**Note:** The IBM 7857-017 modem has two telephone line connections on the back of the unit. One is marked **LL** (for leased line), and the other is marked **PTSN** (for Public Telephone Switched Network). The Electronic Service Agent expects to use the modem on the public network, so the telephone line should attach to the PTSN connector.

3. You have completed the modem configuration.

---

## Configuring the 7852-400 Modem

The 7852 Model 400 is one of the recommended modem choices for the Electronic Service Agent. From the factory, there are DIP switches on the side of the modem that need to be set to make the asynchronous mode the default mode. Switch 12 needs to be set to the off (down) position for asynchronous mode. Switch 11 needs to be set to the on (up) position to enable AT Responses. If you want to enable the auto-answer capability of the 7852-400 modem to perform remote dial-in to the NAS Gateway 500, Switch 5 needs to be set to the on (up) position to enable auto-answer. If your security requirements do not allow remote dial-in, switch 5 needs to be set to the off (down) position to disable auto-answer. See “IBM 7852-400 DIP switch settings” on page 257 for proper setting of switches.

To set up and initialize the 7852-400 for operation:

1. Set switches 5, 11 and 12 to their appropriate position.
2. Connect the RS232 cable to the modem and to a serial port.
3. Connect the telephone cable (sent with the modem) to the modem connector labeled LINE (middle connector), and to the telephone wall jack.
4. Connect the modem power cable to the modem and the transformer to the building power.
5. Power-on the modem (switch in rear).

---

## Configuring the 7857-017 or 7858-336 Modem

The 7857 is one of the recommended modem choices for the Electronic Service Agent. The 7858-336 is the replacement modem for the 7857. These procedures aid in the proper configuration of the 7857-017 or 7858-336, or set a known configuration state.

To set up and initialize the 7857-017 or 7858-336 for operation:

1. Connect the RS232 cable to the modem and to a serial port.
2. Connect the telephone cable (sent with the modem) to the modem connector labeled PSTN, and to the telephone wall jack.
3. Connect the modem power cable to building power.
4. Power-on the modem.
5. Wait for the main display panel.

Use the following procedure to place the modem in a known configuration. After the modem is powered on and local tests have completed, there should be two lines of configuration information displayed on the modem LCD screen.

1. Press ↓ 12 times until the CONFIGURATIONS message is displayed.

CONFIGURATIONS D12

2. Press → until the Select Factory message is displayed.

CONFIGURATIONS D12

Select **Factory** .

3. Press **Enter** to select the Factory configuration option. Press ↑ until 0 is displayed.

CONFIGURATIONS D12

Select **Factory 0**.

4. Press **Enter** to load the predefined factory configuration 0.

```
IBM 7857 AT CMD aa 
td_rd_dsr_ec  11_
```

5. Press ↓ seven times until the S-REGISTER message is displayed.  
S-REGISTER D7
6. Press → until the message Ring to answer on is displayed.  
S-REGISTER D7  
Ring to answ. On=2\_
7. Press **Enter** to select Ring to answer on.  
S-REGISTER D7  
Ring to answ. On=\_
8. Press ↑ until 0 is displayed.  
S-REGISTER D7  
Ring to answ. On=0
9. Press **Enter** to set Auto Answer to 0.  
S-REGISTER D7
10. Press ↓ five times until the CONFIGURATIONS message is displayed.  
CONFIGURATIONS D12
11. Press → three times until the Store User Conf. message is displayed.  
CONFIGURATIONS D12  
Store User Conf.\_
12. Press **Enter** to select the Store User Configuration option. Press ↑ until 0 is displayed.  
CONFIGURATIONS D12  
Store User Conf. 0
13. Press **Enter** to select location 0.
14. Press **Enter** to save current configuration into User 0.  
CONFIGURATIONS D12
15. Press **Enter** to return to main display panel.  
IBM 7857 AT CMD aa\_  
td\_rd\_dsr\_ec  11\_     = Shows LCD as on.

The above setup places the 7857 or 7858 modem into the proper configuration for use with the Dialer that is used for the Electronic Service Agent and the service processor.

**Note:** The modem initialization strings provided are on an AS IS basis. Although they have been tested in a typical AIX environment they might have to be modified depending on the actual setup and configuration of your environment.

---

## IBM 7852-400 DIP switch settings

If you are using a 7852-400 modem to enable Electronic Service Agent and service processor communications, for proper operation, the DIP switches must be set according to the following table:

Switch	Position	Function
1	Up	Force DTR
2	Up	Flow control &E4
3	Down	Result codes enabled
4	Down	Modem emulation disabled
5	Up	Auto answer enabled

Switch	Position	Function
6	Up	Maximum throughput enabled
7	Up	RTS normal functions
8	Down	Enable command mode
9	Down	Remote digital loopback test enabled
10	Up	Dial-up line enabled
11	*Up	AT responses enabled (extended responses disabled)
12	*Down	Asynchronous operation
13	Up	28.8-KB line speed
14	Up	
15	Up	CD and DSR normal functions
16	Up	2-wire leased line enabled

\* Only switches 11 and 12 are changed from the factory default settings.



---

## Appendix B. Command shortcuts using SMIT fastpath and WebSM

This appendix contains the following sections:

- “Managing administrators” on page 260
- “Managing applications (TSM, TSANM, TSRM, SNMP)” on page 261
- “Managing client access” on page 265
  - “Managing local file access users and groups” on page 265
  - “Directories” on page 267
    - “NIS SMIT fastpaths and WebSM access” on page 267
    - “NIS+ command SMIT fastpaths and WebSM access” on page 269
    - “LDAP SMIT fastpaths and WebSM access” on page 270
- “Managing clustering” on page 271
- “Managing devices” on page 273
- “Managing file serving” on page 275
  - “FTP command SMIT fastpaths and WebSM access” on page 275
  - “HTTP command SMIT fastpaths and WebSM access” on page 275
  - “NFS command SMIT fastpaths and WebSM access” on page 276
  - “CIFS command SMIT fastpaths and WebSM access” on page 279
- “Managing the network” on page 281
- “Managing security” on page 284
- “Managing the system” on page 285
  - “Backup and recovery SMIT fastpaths and WebSM access” on page 285
  - “Boot and shutdown SMIT fastpaths and WebSM access” on page 285
  - “Date and time SMIT fastpaths and WebSM access” on page 285
  - “Problem determination SMIT fastpaths and WebSM access” on page 286
  - “System information command SMIT fastpaths and WebSM access” on page 287
- “Managing volumes, Remote Mirroring, and snapshots” on page 289
  - “Managing local volumes” on page 289
  - “Managing remotely mirrored volumes” on page 291
  - “Snapshot SMIT fastpaths and WebSM access” on page 293

## Managing administrators

Table 17. Administrator SMIT fastpaths and WebSM access

Command	Description	
mknasadm	Add administrative user. (Based on mkuser)	
	SMIT fastpath	<b>smit mknasadm</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Administrators</b> → <b>Overview and Tasks</b> → <b>Create a NAS Administrator</b>
lsnasadm	List NAS administrators. (Based on lsuser)	
	SMIT fastpath	<b>smit lsnasadm</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Administrators</b> → <b>All NAS Administrators</b>
lsnasadm -f	Show characteristics of an administrator.	
	SMIT fastpath	<b>smit lsnasadm f</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Administrators</b> → <b>All Administrators</b> →select an administrator→ <b>Properties</b>
pwdadm	Change administrator password.	
	SMIT fastpath	<b>smit passwdadm</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Administrators</b> → <b>All Administrators</b> →select an administrator→ <b>Change Password</b>

## Managing applications (TSM, TSANM, TSRM, SNMP)

Table 18. TSM, TSANM, TSRM and SNMP SMIT fastpaths and WebSM access

Command	Description	
tsrmasetconfig	Configure communication parameters for TSRM Agent.	
	SMIT fastpath	<b>smit tsrmasetconfig</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSRM</b> → <b>Configure TSRM Agent</b> →specify settings→ <b>OK</b>
tsrmasetstate	Start or stop TSRM Agent.	
	SMIT fastpath	<b>smit tsrmasetstate</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSRM</b> → <b>Start or Stop TSRM Agent</b> →specify settings→ <b>OK</b>
tsrmasetboot	Change or show boot state of TSRM Agent.	
	SMIT fastpath	<b>smit tsrmasetboot</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSRM</b> → <b>TSRM Agent Boot Options</b> →specify settings→ <b>OK</b>

Table 18. TSM, TSANM, TSRM and SNMP SMIT fastpaths and WebSM access (continued)

Command	Description	
tsanmasetconfig	Configure communication parameters for TSANM Agent.	
	SMIT fastpath	<b>smit tsanmasetconfig</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSANM</b> → <b>Configure TSANM Agent Password</b> →specify settings→ <b>OK</b>
tsanmasetstate	Start or stop TSANM Agent.	
	SMIT fastpath	<b>smit tsanmasetstate</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSANM</b> → <b>Start or Stop TSANM Agent</b> →specify settings→ <b>OK</b>
tsanmasetpass	Set password for Tivoli SAN Manager Agent.	
	SMIT fastpath	<b>smit tsanmasetpass</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSANM</b> → <b>Configure TSANM Agent Password</b> →specify settings→ <b>OK</b>
tsanmasetboot	Set password for Tivoli SAN Manager Agent.	
	SMIT fastpath	<b>smit tsanmasetboot</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSANM</b> → <b>TSANM Agent Boot Option</b> →specify settings→ <b>OK</b>

Table 18. TSM, TSANM, TSRM and SNMP SMIT fastpaths and WebSM access (continued)

Command	Description	
tsmcsetconfig	Configure communication parameters for TSM Client	
	SMIT fastpath	<b>smit tsmcsetconfig</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Configure TSM Client</b> →specify settings→ <b>OK</b>
tsmcbackup -i	TSM Backup - Incremental	
	SMIT fastpath	<b>smit tsmcbackupi</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Backup Using TSM Client</b> →specify settings→ <b>OK</b>
tsmcbackup -s	TSM Backup - Selective	
	SMIT fastpath	<b>smit tsmcbackups</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Backup Using TSM Client</b> →specify settings→ <b>OK</b>
tsmcrestore -f	TSM Restore - Filesystem	
	SMIT fastpath	<b>smit tsmcrestorefs</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Recover Using TSM Client</b> →specify settings→ <b>OK</b>
tsmcrestore -l	TSM Restore - File	
	SMIT fastpath	<b>smit tsmcrestoref</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Recover Using TSM Client</b> →specify settings→ <b>OK</b>
tsmsasetconfig	Configure communication parameters for TSM storage agent	
	SMIT fastpath	<b>smit tsmsasetconfig</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Configure TSM Storage Agent</b> →specify settings→ <b>OK</b>
tsmsasetstate	Start / Stop TSM storage agent	
	SMIT fastpath	<b>smit tsmsasetstate</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>Start or Stop TSM Storage Agent</b> →specify settings→ <b>OK</b>
tsmsasetboot	Change Boot State of TSM storage agent	
	SMIT fastpath	<b>smit tsmsasetboot</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Node (Server IP Address)</b> → <b>Applications</b> → <b>TSM</b> → <b>TSM Storage Agent Boot Option</b> →specify settings→ <b>OK</b>

Table 18. TSM, TSANM, TSRM and SNMP SMIT fastpaths and WebSM access (continued)

Command	Description	
snmpinfo	Request values of Management Information Base (MIB) variables managed by a Simple Network Management Protocol (SNMP) agent.	
	SMIT fastpath	<b>smit snmpinfo_get</b>
	WebSM	<b>NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Get SNMP Information</b>
snmpinfo	Modify values of Management Information Base (MIB) variables managed by a Simple Network Management Protocol (SNMP) agent.	
	SMIT fastpath	<b>smit snmpinfo_set,</b>
	WebSM	<b>NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Set SNMP Information</b>
snmpinfo	Dump SNMP information.	
	SMIT fastpath	<b>smit snmpinfo_dump</b>
	WebSM	<b>NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Dump SNMP Information</b>
snmpinfo	Start SNMP.	
	SMIT fastpath	<b>smit stsnmpd</b>
	WebSM	<b>NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Start SNMP service</b>
snmpinfo	Stop SNMP.	
	SMIT fastpath	<b>smit spsnmpd</b>
	WebSM	<b>NAS Management→NAS System→Node (Server IP Address)→Applications→SNMP→Stop SNMP service</b>

## Managing client access

### Managing local file access users and groups

Table 19. File access user SMIT fastpaths and WebSM access

Command	Description	
mknasuser	Add file access user.	
	SMIT fastpath	<b>smit mknasuser</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;Overview and Tasks&gt;Manage users&gt;Add</b>
lsnasuser	List file access users.	
	SMIT fastpath	<b>smit lsnasuser</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;All Users</b>
chuser	Change or show characteristics of a user.	
	SMIT fastpath	<b>smit chnasuser</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;All Users&gt;select the user&gt;Properties</b>
pwdadm	Change a file access user's password.	
	SMIT fastpath	<b>smit passwduser</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;All Users&gt;select the user&gt;Change Password</b>
rmuser	Remove a user. (Based on rmuser)	
	SMIT fastpath	<b>smit rmnasuser</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;Overview and Tasks&gt;Manage users&gt;Delete</b>
mkgroup	Add a group.	
	SMIT fastpath	<b>smit mkgroup</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;Overview and Tasks&gt;Create a new Group</b>
lsgroup	List all groups	
	SMIT fastpath	<b>smit lsgroup</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;Overview and Tasks&gt;All Groups</b>
chgrpmem	Change membership of a group.	
	SMIT fastpath	<b>smit chgroup</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Client Access&gt;Overview and Tasks&gt;All Groups&gt;(right-click a group)</b>

Table 19. File access user SMIT fastpaths and WebSM access (continued)

Command	Description	
rmgroup	Remove a group.	
	SMIT fastpath	<b>smit rmgroup</b>
	WebSM	<b>NAS Management→NAS System→Client Access→Overview and Tasks→All Groups→(right-click a group)</b>



## Directories

This section contains the following information:

- “NIS SMIT fastpaths and WebSM access”
- “NIS+ command SMIT fastpaths and WebSM access” on page 269
- “LDAP SMIT fastpaths and WebSM access” on page 270

### NIS SMIT fastpaths and WebSM access

Table 20. NIS SMIT fastpaths and WebSM access

Command	Description	
mkclient	Configure host as NIS client. This starts the ypbind daemon.	
	SMIT fastpath	<b>smit mkclient</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS</b> → <b>NIS Client</b> →(right-click the client). Select <b>Open</b> from the <b>Selected</b> menu.
chclient	Reconfigure host as a NIS client.	
	SMIT fastpath	<b>smit chclient</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS</b> → <b>NIS Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
chypdom	Change current domain name of the system.	
	SMIT fastpath	<b>smit chypdom</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS</b> → <b>NIS Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
ypbind	Configure binding of client to server.	
	SMIT fastpath	<b>smit ypbind</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS</b> → <b>NIS Client</b> →(right-click the client). Select <b>Bind Client to a Server</b> from the Selected menu.
ypcat	Prints a NIS map.	
	SMIT fastpath	<b>smit ypcat</b>
	WebSM	N/A
ypmatch	Displays value of keys in NIS map.	
	SMIT fastpath	<b>smit ypmatch</b>
	WebSM	N/A

Table 20. NIS SMIT fastpaths and WebSM access (continued)

Command	Description	
yppoll	Display order number of NIS map in use on server.	
	SMIT fastpath	<b>smit yppoll</b>
	WebSM	N/A
ypset	Bind NIS client to specific server.	
	SMIT fastpath	<b>smit ypset</b>
	WebSM	N/A
ypwhich	Identify current NIS server.	
	SMIT fastpath	<b>smit ypwhich</b>
	WebSM	N/A
	Identify specific NIS server.	
	SMIT fastpath	<b>smit ypwhichs</b>
	WebSM	N/A
	Identify master NIS server.	
	SMIT fastpath	<b>smit ypwhichm</b>
	WebSM	N/A
rmyp	Remove NIS client configuration from host.	
	SMIT fastpath	<b>smit rmyp</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS</b> → <b>NIS Client</b> →(right-click the client). Select <b>Stop Configured NIS Daemons</b> from the Selected menu.
yppasswd	Change or install network password in NIS.	
	SMIT fastpath	<b>smit yppasswd</b>
	WebSM	N/A
chypserver	Adds or deletes IP address to search for NIS connection.	
	SMIT fastpath	<b>smit chypserver</b>
	WebSM	N/A

## NIS+ command SMIT fastpaths and WebSM access

Table 21. NIS+ command SMIT fastpaths and WebSM access

Command	Description	
nisinit	Initialize system as NIS+ client.	
	SMIT fastpath	<b>smit nisp_nisd_start</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
nisclient	Configure this host as a NIS+ client.	
	SMIT fastpath	<b>smit nisclient</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
nisclient -D	Remove NIS+ Client Configuration from this host.	
	SMIT fastpath	<b>smit nisp_unclient</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
nisaddcred	NIS+ credential administration.	
	SMIT fastpath	<b>smit nisp_creds</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Open</b> from the Selected menu.
mk_nisd	Start NIS+ daemon.	
	SMIT fastpath	<b>smit nisp_nisd_start</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Start NIS+ Daemons</b> from the Selected menu.
rm_nisd	Stop NIS+ daemon.	
	SMIT fastpath	<b>smit nisp_nisd_stop</b>
	WebSM	N/A
nisdefaults	Display default values in the namespace.	
	SMIT fastpath	<b>smit nisdefaults</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Directory Services</b> → <b>NIS+</b> → <b>NIS+ Client</b> →(right-click the client). Select <b>Stop NIS+ Daemons</b> from the Selected menu.
nistest	Return the state of the NIS+ namespace.	
	SMIT fastpath	<b>smit show_namespace</b>
	WebSM	N/A
nischttl	Change Time to Live values of NIS+ objects or entries.	
	SMIT fastpath	<b>smit nischttl</b>
	WebSM	N/A

Table 21. NIS+ command SMIT fastpaths and WebSM access (continued)

Command	Description	
nisls	List contents of NIS+ directory.	
	SMIT fastpath	<b>smit nisls</b>
	WebSM	N/A
niscat	Display contents of NIS+ table.	
	SMIT fastpath	<b>smit niscat</b>
	WebSM	N/A
nismatch	Show values in NIS+ tables.	
	SMIT fastpath	<b>smit nismatch</b>
	WebSM	N/A
nisgrep	Search NIS+ tables.	
	SMIT fastpath	<b>smit nisgrep</b>
	WebSM	N/A

## LDAP SMIT fastpaths and WebSM access

Table 22. LDAP SMIT fastpaths and WebSM access

Command	Description	
mksecdap	Configure LDAP client	
	SMIT fastpath	<b>smit mksecdap</b>
	WebSM	N/A
mksecdap -c -U	Unconfigure an LDAP client.	
	SMIT fastpath	<b>smit mksecdapu</b>
	WebSM	N/A

## Managing clustering

Table 23. Clustering fastpaths and WebSM access

Command	Description	
clnasencluster	Start cluster services on all nodes.	
	SMIT fastpath	<b>smit clnasencluster</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Enable cluster</b>
clnasdiscluster	Stop cluster services on all nodes.	
	SMIT fastpath	<b>smit clnasdiscluster</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Disable cluster</b>
clnasnodestate	Show cluster server state.	
	SMIT fastpath	<b>smit clnasnodestate</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Show server state</b>
clnasisconfigd	Verify cluster	
	SMIT fastpath	<b>smit clnasisconfigd</b>
	WebSM	<b>NAS Management→NAS System→NAS Cluster Management→Verify cluster</b>
clnassync	Synchronize cluster.	
	SMIT fastpath	<b>smit clnassync</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Synchronize cluster</b>
clnasshowvol	Show volumes being served.	
	SMIT fastpath	<b>smit clnasshowvol</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Show volumes being served</b>
clnasrelocate	Relocate volumes.	
	SMIT fastpath	<b>smit clnasrelocate</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Relocate volumes</b>
clnasenvol	Enable a volume in the cluster.	
	SMIT fastpath	<b>smit clnasenvol</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Enable Volumes</b>
clnasdisvol	Disable a volume in the cluster.	
	SMIT fastpath	<b>smit clnasdisvol</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Disable Volumes</b>
clnasennode	Enable server in cluster.	
	SMIT fastpath	<b>smit clnasennode</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Enable server</b>

Table 23. Clustering fastpaths and WebSM access (continued)

Command	Description	
clnasdisnode	Disable server in cluster.	
	SMIT fastpath	<b>smit clnasdisnode</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Disable server</b>
clnasengroup	Enable a resource group.	
	SMIT fastpath	<b>smit clnasengroup</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Enable resource group</b>
clnasdisgroup	Disable a resource group.	
	SMIT fastpath	<b>smit clnasdisgroup</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Disable resource group</b>
clnasmvservice	Move service to another adapter.	
	SMIT fastpath	<b>smit clnasmvservice</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Move service</b>
clnasdelcluster	Delete cluster.	
	SMIT fastpath	<b>smit clnasdelcluster</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Delete cluster</b>
clnasviewlog	View cluster log.	
	SMIT fastpath	<b>smit clnasviewlog</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→View log</b>
clnasshowcluster	View a cluster.	
	SMIT fastpath	<b>smit clnasshowcluster</b>
	WebSM	<b>NAS Management→NAS System→Cluster Management→Show configuration</b>

## Managing devices

Table 24. Devices command SMIT fastpaths and WebSM access

Command	Description	
cfgmgr	Configure new devices.	
	SMIT fastpath	<b>smit cfgmgr</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Overview and Tasks</b> → <b>Discover devices that were powered on after the last system restart</b>
lscfg	Show system device configuration.	
	SMIT fastpath	<b>smit lscfg</b>
	WebSM	
lspvol	Show configured disks.	
	SMIT fastpath	<b>smit lspvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Disks</b>
lspvol (specific)	Show configured disks (specific).	
	SMIT fastpath	<b>smit lspvoldisk</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Disks</b> → (right-click a disk)→ <b>Attributes</b> .
rmdev	Unconfigure devices.	
	SMIT fastpath	<b>smit rmdev</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Disks</b> → (right-click a disk)→ <b>Take Offline (Make Defined) or Delete</b> .
chpvol	Clear NAS volume information from the disk.	
	SMIT fastpath	<b>smit chpvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Disks</b> →(right-click a disk)→ <b>Clear Volume Information</b> .
chpgeovol	Clear NAS volume information from the disk.	
	SMIT fastpath	<b>smit chpgeovol</b>
	WebSM	

Table 24. Devices command SMIT fastpaths and WebSM access (continued)

Command	Description	
mklinkagg	Create a link aggregation device.	
	SMIT fastpath	<b>smit mklinkagg</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Communication</b> → <b>Overview and Tasks</b> → <b>Create a Link Aggregation</b> .
chlinkagg	Change attributes of a link aggregation device.	
	SMIT fastpath	<b>smit chlinkagg</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Communication</b> → <b>Link Aggregation</b> →(right-click a link aggregation)→ <b>Change</b> .
rmlinkagg	Remove a link aggregation device.	
	SMIT fastpath	<b>smit rmlinkagg</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Communication</b> → <b>Link Aggregation</b> →(right-click a link aggregation)→ <b>Delete</b> .
lslinkagg	List attributes of a link aggregation device.	
	SMIT fastpath	<b>smit lslinkagg</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>Devices</b> → <b>Communication</b> → <b>ALL Link Aggregations</b> →(right-click a link aggregation)→ <b>Properties</b> .



## Managing file serving

This section contains the following information:

- “FTP command SMIT fastpaths and WebSM access”
- “HTTP command SMIT fastpaths and WebSM access”
- “NFS command SMIT fastpaths and WebSM access” on page 276

### FTP command SMIT fastpaths and WebSM access

Table 25. FTP command SMIT fastpaths and WebSM access

Command	Description	
mkanonftp	Create an anonymous user account on the system to support file transfers from the server without requiring a password.	
	SMIT fastpath	<b>smit mkanonftp</b>
	WebSM	<b>NAS Management→NAS System→File Serving→FTP→Create FTP user login</b>
mkanonftp.user	Create an anonymous login account for a named user.	
	SMIT fastpath	<b>smit mkanonftp.user</b>
	WebSM	<b>NAS Management→NAS System→File Serving→FTP→Create / Enable FTP User Login</b>

### HTTP command SMIT fastpaths and WebSM access

Table 26. HTTP command SMIT fastpaths and WebSM access

Command	Description	
htpasswd	Authenticate users.	
	SMIT fastpath	<b>htpasswd</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Authenticate Users</b>
adhtaccess	Configure HTTP access.	
	SMIT fastpath	<b>adhtaccess</b>
	WebSM	N/A
N/A	Manage HTTP service.	
	SMIT fastpath	<b>http</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→(select a task)</b>
apachectl start	Start HTTP service.	
	SMIT fastpath	<b>smit apachectl_start</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Start HTTP service</b>
apachectl restart	Restart HTTP service.	
	SMIT fastpath	<b>smit apachectl_restart</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Restart HTTP service</b>

Table 26. HTTP command SMIT fastpaths and WebSM access (continued)

Command	Description	
apachectl stop	Stop HTTP service.	
	SMIT fastpath	<b>smit apachectl_stop</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Stop HTTP service</b>
adminctl start	Start HTTP administration service.	
	SMIT fastpath	<b>smit adminctl_start</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Start HTTP Administration service</b>
adminctl restart	Restart HTTP administration service.	
	SMIT fastpath	<b>smit adminctl_restart</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Restart HTTP Administration service</b>
adminctl stop	Stop HTTP administration service.	
	SMIT fastpath	<b>smit adminctl_stop</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→Stop HTTP Administration service</b>
lshttp	View HTTP configuration.	
	SMIT fastpath	<b>smit lshttp</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→View HTTP Configuration</b>
lshttplogs	View HTTP logs.	
	SMIT fastpath	<b>smit lshttplogs</b>
	WebSM	<b>NAS Management→NAS System→File Serving→HTTP→View HTTP logs</b>

## NFS command SMIT fastpaths and WebSM access

Table 27. NFS command SMIT fastpaths and WebSM access

Command	Description	
mknfs	Start NFS.	
	SMIT fastpath	<b>smit mknfs</b>
	WebSM	<b>NAS Management→NAS System→File Serving→Network File System. From the Network File Systems menu, select <b>Start NFS</b>.</b>
rmnfs	Stop NFS.	
	SMIT fastpath	<b>smit rmnfs</b>
	WebSM	<b>NAS Management→NAS System→File Serving→Network File System. From the Network File Systems menu, select <b>Stop NFS</b>.</b>

Table 27. NFS command SMIT fastpaths and WebSM access (continued)

Command	Description	
chnfs	Change number of daemons.	
	SMIT fastpath	<b>smit chnfs</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File System</b> . From the Network File Systems menu, select <b>Change Number of NFS Daemons</b> .
mknasnfsexp	Add a directory to exports list.	
	SMIT fastpath	<b>smit mknasnfsexp</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Exported Directories</b> . From the Directories menu, select <b>New</b> .
rmnasnfsexp	Unexport and remove a directory to exports list.	
	SMIT fastpath	<b>smit rmnasnfsexp</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Exported Directories</b> →(right-click a directory)→ <b>Remove Export</b> .
chnasnfsexp	Show or change attributes of exported directory.	
	SMIT fastpath	<b>smit chnasnfsexp</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Exported Directories</b> →(right-click a directory)→ <b>Properties</b>
exportnasfs	Display currently exported volumes.	
	SMIT fastpath	<b>smit exportnasfs</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File System</b>
	Export all volumes.	
	SMIT fastpath	<b>smit exportnasfsea</b>
	WebSM	N/A
	Export specific volume.	
	SMIT fastpath	<b>smit exportnasfses</b>
	WebSM	N/A
	Unexport all volumes.	
	SMIT fastpath	<b>smit exportnasfsua</b>
	WebSM	N/A
	Unexport specific volume.	
	SMIT fastpath	<b>smit exportnasfsus</b>
	WebSM	N/A

Table 27. NFS command SMIT fastpaths and WebSM access (continued)

Command	Description	
showmount	Display a list of all clients with remotely mounted filesystems.	
	SMIT fastpath	<b>smit showmount</b>
	WebSM	N/A
mkpcnfs	Start PC NFS.	
	SMIT fastpath	<b>smit mkpcnfs</b>
	WebSM	N/A
rmpcnfs	Stop PC NFS.	
	SMIT fastpath	<b>smit rmpcnfs</b>
	WebSM	N/A

## CIFS command SMIT fastpaths and WebSM access

Table 28. CIFS command SMIT fastpaths and WebSM access

Command	Description
net	Start server.
	SMIT fastpath <b>smit smbadminstart</b>
	WebSM <b>NAS Management&gt;NAS System &gt;File Serving&gt;CIFS&gt;Overview and Tasks&gt;Start local CIFS Server Operations</b>
	Stop server
	SMIT fastpath <b>smit smbadminstop</b>
	WebSM <b>NAS Management&gt;NAS System &gt;File Serving&gt;CIFS&gt;Overview and Tasks&gt;Stop local CIFS Server Operations</b>
	Server status
	SMIT fastpath <b>smit smbadminstatu</b>
	WebSM <b>NAS Management&gt;NAS System &gt;File Serving&gt;CIFS&gt;CIFS Server</b>
	Server statistics.
	SMIT fastpath <b>smit smbadminstats</b>
	WebSM <b>NAS Management&gt;NAS System &gt;File Serving&gt;CIFS-&gt;CIFS Server-&gt;(right-click a server)-&gt;Show Server Statistics</b>
	Basic setup.
	SMIT fastpath <b>smit smbcfghatt</b>
	WebSM <b>NAS Management&gt;NAS System &gt;File Serving&gt;CIFS&gt;Overview and Tasks&gt;CIFS Wizard</b>
	Authentication
	SMIT fastpath <b>smit smbcfgauth</b>
	WebSM N/A
	Remote authentication options
	SMIT fastpath <b>smit smbcfgauthremote</b>
	WebSM N/A
	Resource limits
	SMIT fastpath <b>smit smbcfgresi</b>
	WebSM N/A

Table 28. CIFS command SMIT fastpaths and WebSM access (continued)

Command	Description	
net	Network logon.	
	SMIT fastpath	<b>smit smbcfgauthnetlog</b>
	WebSM	N/A
	File server characteristics	
	SMIT fastpath	<b>smit smbcfgflags1</b>
	WebSM	N/A
	Work with CIFS file shares	
	SMIT fastpath	<b>smit smbsrvres</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>CIFS</b> → <b>CIFS Server</b> →(right-click a server)→ <b>New</b> → <b>File System Share</b>
	List all CIFS users	
	SMIT fastpath	<b>smit smbcfgusr</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>CIFS</b> → <b>Overview and Tasks</b> → <b>User Administration</b>

## Managing the network

Table 29. Network SMIT fastpaths and WebSM access

Command	Description	
arp	Display and modify address resolution.	
	SMIT fastpath	N/A
	WebSM	N/A
autoconf6	Automatically configure IPv6 network interfaces at boot time.	
	SMIT fastpath	N/A
	WebSM	N/A
chauthent	Change the configured authentication methods for the system.	
	SMIT fastpath	N/A
	WebSM	N/A
hostname	Set or display the name of the current host system.	
	SMIT fastpath	<b>smit hostname</b>
	WebSM	<b>NAS Management→NAS System →Node(Server IP Address)→Network→TCP/IP (IPv4 and IPv6)→Protocol Configuration→Set up basic TCP/IP configuration</b>
ifconfig	Configure or display network interface parameters for a network using TCP/IP.	
	SMIT fastpath	<b>smit inet</b>
	WebSM	<b>NAS Management→NAS System →Node(Server IP Address)→Network→TCP/IP (IPv4 and IPv6)→Network Interfaces</b>
ipfilter	Extract different operation headers from an ipreport output file and display them in a table.	
	SMIT fastpath	N/A
	WebSM	N/A
ipreport	Generate a packet trace report from the specified packet trace file.	
	SMIT fastpath	N/A
	WebSM	N/A
logger	Make entries in the system log.	
	SMIT fastpath	N/A
	WebSM	N/A
logout	Stop all processes on a port.	
	SMIT fastpath	N/A
	WebSM	N/A
lsauthent	List the authentication methods currently configured on the system.	
	SMIT fastpath	N/A
	WebSM	N/A

Table 29. Network SMIT fastpaths and WebSM access (continued)

Command	Description	
lssrc	Get the status of a subsystem, a group of subsystems, or a subserver.	
	SMIT fastpath	<b>smit inet</b>
	WebSM	<b>NAS Management→NAS System→Node(Server IP Address)→Network→TCP/IP (IPv4 and IPv6)→Subsystems</b>
mktcpip	Set the required values for starting TCP/IP on a host.	
	SMIT fastpath	<b>smit mktcpip</b>
	WebSM	<b>NAS Management→NAS System→Node(Server IP address)→Network→TCP/IP (IPv4 and IPv6)→Protocol Configuration→Set up basic TCP/IP configuration.</b>
netstat	Show network statistics.	
	SMIT fastpath	N/A
	WebSM	N/A
ping	Send an echo request to a network host.	
	SMIT fastpath	N/A
	WebSM	N/A
namerslv	Directly manipulate domain name server entries for local resolver routines in the system configuration database.	
	SMIT fastpath	<b>smit namerslv</b>
	WebSM	N/A
nfso	Manage Network File System (NFS) tuning parameters.	
	SMIT fastpath	N/A
	WebSM	N/A
no	Manage network tuning parameters.	
	SMIT fastpath	N/A
	WebSM	N/A
refresh	Request a refresh of a subsystem or group of subsystems.	
	SMIT fastpath	N/A
	WebSM	N/A
startsrc	Start a subsystem, a group of subsystems, or a subserver.	
	SMIT fastpath	There are many fastpaths.
	WebSM	<b>NAS Management→NAS System→Node(Server IP Address)→Network→TCP/IP (IPv4 and IPv6)→Subsystems→(right-click subsystem)→Activate</b>
stopsrc	Stop a subsystem, a group of subsystems, or a subserver.	
	SMIT fastpath	There are many fastpaths.
	WebSM	<b>NAS Management→NAS System→Node(Server IP Address)→Network→TCP/IP (IPv4 and IPv6)→Subsystems→(right-click subsystem)→Deactivate</b>



Table 29. Network SMIT fastpaths and WebSM access (continued)

Command	Description	
traceroute	Print the route that IP packets take to a network host.	
	SMIT fastpath	N/A
	WebSM	N/A
mkroute	Add a static route.	
	SMIT fastpath	<b>smit mkroute</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;*Node IP*&gt;Network&gt;Overview and Tasks&gt;Static route wizard</b>
rmroute	Delete a static route on the local node, its peer node, or both.	
	SMIT fastpath	<b>smit rmroute</b>
	WebSM	N/A
lsroute	List the static routes on the local node, its peer node, or both.	
	SMIT fastpath	<b>smit lsroute</b>
	WebSM	N/A

## Managing security

### Secure NFS command SMIT fastpaths and WebSM access

Table 30. Secure NFS command SMIT fastpaths and WebSM access

Command	Description	
mkkeyserv	Starts the keyserv daemon.	
	SMIT fastpath	<b>smit mkkeyserv</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>
rmkeyserv	Stops the keyserv daemon.	
	SMIT fastpath	<b>smit rmkeyserv</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>
newkey	Establish public keys	
	SMIT fastpath	<b>smit newkey</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>
keylogin	Decrypts and stores user key.	
	SMIT fastpath	<b>smit keylogin</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>
keylogout	Deletes user key.	
	SMIT fastpath	<b>smit keylogout</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>
chkey	Change encrypting key.	
	SMIT fastpath	<b>smit chkey</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>File Serving</b> → <b>Network File Systems</b> . From the Menu Bar, right-click <b>FileSystem</b> and select <b>Configure Secure NFS</b>

---

## Managing the system

This section contains the following information:

### Backup and recovery SMIT fastpaths and WebSM access

Table 31. Backup and recovery SMIT fastpaths and WebSM access

Command	Description	
mknasb	Create configuration file backup.	
	SMIT fastpath	<b>smit mknasb</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>System Environment</b> → <b>Backup and Restore</b> → <b>Backup Configuration Files</b>
restnasb	Restore configuration file backup.	
	SMIT fastpath	<b>smit restnasb</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>System Environment</b> → <b>Backup and Restore</b> → <b>Restore Configuration Files</b>

### Boot and shutdown SMIT fastpaths and WebSM access

Table 32. Boot and shutdown SMIT fastpaths and WebSM access

Command	Description	
shutdown	Shutdown	
	SMIT fastpath	<b>smit shutdown</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>System Environment</b> → <b>Overview and Tasks</b> → <b>Shutdown</b>
chreboot	Change reboot options.	
	SMIT fastpath	<b>smit chreboot</b>
	WebSM	N/A

### Date and time SMIT fastpaths and WebSM access

Table 33. Date and time SMIT fastpaths and WebSM access

Command	Description	
chtz	Change time zone using system-defined values.	
	SMIT fastpath	<b>smit chtz</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>System Environment</b> → <b>Settings</b> , then double-click the <b>Date and Time</b> icon.
	SMIT fastpath	<b>smit date_time</b>
	WebSM	N/A
chtz	Change time zone using user-supplied values	
	SMIT fastpath	<b>smit chtz</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <i>Node</i> → <b>System Environment</b> → <b>Settings</b> , then double-click the <b>Date and Time</b> icon.

Table 33. Date and time SMIT fastpaths and WebSM access (continued)

Command	Description	
date	Change or show date and time.	
	SMIT fastpath	<b>smit date</b>
	WebSM	<b>NAS Management&gt;NAS System&gt;Node&gt;System Environment&gt;Settings</b> , then double-click the <b>Date and Time</b>

## Problem determination SMIT fastpaths and WebSM access

Table 34. Problem determination SMIT fastpaths and WebSM access

Command	Description	
snap	Collect debugging data.	
	SMIT fastpath	<b>smit snap</b>
	WebSM	N/A
sysdumpdev	Always allow system dump.	
	SMIT fastpath	<b>smit sysdumpdev_allow</b>
	WebSM	N/A
	System dump compression.	
	SMIT fastpath	<b>smit sysdumpdev_comp</b>
	WebSM	N/A
diag	Hardware problem determination	
	SMIT fastpath	<b>smit diag</b>
	WebSM	N/A
trace	Tracing:	
	Start a trace	
	SMIT fastpath	<b>smit trcstart</b>
	WebSM	N/A
trcstop	Stop a trace	
	SMIT fastpath	<b>smit trcstop</b>
	WebSM	N/A
trcrpt	Generate a trace report.	
	SMIT fastpath	<b>smit trcrpt</b>
	WebSM	N/A
trcevgrp	Manage group events	
	SMIT fastpath	<b>smit grpmenu</b>
	WebSM	N/A

## System information command SMIT fastpaths and WebSM access

Table 35. System information command SMIT fastpaths and WebSM access

Command	Description	
showlog	Show command log.	
	SMIT fastpath	<b>smit showlog</b>
	WebSM	N/A
filemon	Monitors performance of file system (see also trcon, trcoff, trcstop).	
	SMIT fastpath	<b>smit fsperf</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Monitor a trace of file system and I/O system events</b>
iostat	Reports CPU and I/O statistics.	
	SMIT fastpath	<b>smit iostat</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Show input/output statistics</b>
ps	Show current state of processes.	
	SMIT fastpath	<b>smit ps</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→System Tuning→CPU→All Processes</b>
sar	System activity.	
	SMIT fastpath	<b>smit sar</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Report system activity</b>
svmon	Capture snapshot of virtual memory.	
	SMIT fastpath	N/A
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Capture and analyze a snapshot of virtual memory</b>
topas	System statistics.	
	SMIT fastpath	N/A
	WebSM	N/A
trcon	Start trace collection (see also filemon, trcoff, trcstop).	
	SMIT fastpath	<b>smit trcon</b>
	WebSM	N/A
trcoff	Stop trace collection (see also filemon, trcon, trcstop).	
	SMIT fastpath	<b>smit trcoff</b>
	WebSM	N/A

Table 35. System information command SMIT fastpaths and WebSM access (continued)

Command	Description	
trcstop	Stop tracing (see also filemon, trcon, trcoff).	
	SMIT fastpath	<b>smit trcstop</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Complete filemon processing and generate report</b>
vmstat	Virtual memory statistics.	
	SMIT fastpath	<b>smit vmstat</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Show virtual memory statistics</b>
nfsstat	NFS statistics.	
	SMIT fastpath	<b>smit nfsstat</b>
	WebSM	<b>NAS Management→NAS System →Node→System Environment→System Information→Performance Monitoring→Display statistical information about the Network File System</b>
oslevel	Determine latest installed maintenance.	
	SMIT fastpath	<b>smit oslevel</b>
	WebSM	N/A
naslevel	Determine latest level of NAS Gateway 500.	
	SMIT fastpath	<b>smit naslevel</b>
	WebSM	N/A

## Managing volumes, Remote Mirroring, and snapshots

### Managing local volumes

Table 36. Volumes command SMIT fastpaths and WebSM access

Command	Description	
mkvol	Create a NAS volume.	
	SMIT fastpath	<b>smit mkvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>Overview</b> → <b>Tasks</b> → <b>Create a NAS volume</b>
chvol	Change a NAS volume.	
	SMIT fastpath	<b>smit chvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Change</b>
rmvol	Delete a NAS volume.	
	SMIT fastpath	<b>smit rmvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Delete</b>
defragvol	Defragment a NAS volume.	
	SMIT fastpath	<b>smit defragvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Defragment</b>
expvol	Export a NAS volume.	
	SMIT fastpath	<b>smit expvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Export</b>
impvol	Import a NAS volume.	
	SMIT fastpath	<b>smit impvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>Overview and Tasks</b> →→ <b>Import a NAS Volume</b>
extendvol	Extend the size of a NAS volume.	
	SMIT fastpath	<b>smit extendvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Extend</b> .
syncvol	Synchronize a NAS volume.	
	SMIT fastpath	<b>smit syncvol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> →→ <b>All Volumes</b> →(right-click a volume name)→ <b>Synchronize</b>

Table 36. Volumes command SMIT fastpaths and WebSM access (continued)

Command	Description	
mirvol -u	Unmirror a NAS volume.	
	SMIT fastpath	<b>smit unmirvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Unmirror</b>
replacevol	Replace a NAS volume.	
	SMIT fastpath	<b>smit replacevol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Replace Disk</b>
cpvol	Copy a NAS volume.	
	SMIT fastpath	<b>smit cpvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Copy</b>
mountvol	Mount a NAS volume.	
	SMIT fastpath	<b>smit mountvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Mount</b>
unmountvol	Unmount a NAS volume.	
	SMIT fastpath	<b>smit unmountvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Unmount</b>
mirvol	Mirror a NAS volume.	
	SMIT fastpath	<b>smit mirvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Mirror</b>
lsvol	List attributes of a NAS volume.	
	SMIT fastpath	<b>smit lsvolatt</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Attributes</b>
lsvol	List the known NAS volumes.	
	SMIT fastpath	<b>smit lsvol</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes</b>
volstat	List statistics of a NAS volume.	
	SMIT fastpath	<b>smit volstat</b>
	WebSM	<b>NAS Management→NAS System →Volumes→All Volumes →(right-click a volume name)→Statistics</b>



## Managing remotely mirrored volumes

Table 37. Remote Mirrored volumes command SMIT fastpaths and WebSM access

Command	Description	
mkgeovol	Create NAS remotely mirrored volume	
	SMIT fastpath	<b>smit mkgeovol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>Overview and Tasks</b> → <b>Create a NAS remote mirror volume</b>
lsvol -g	Listing remotely mirrored volumes	
	SMIT fastpath	<b>smit listremotevol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>All Remote Mirror Volumes</b>
rmgeovol	Deleting a remotely mirrored NAS volume	
	SMIT fastpath	<b>smit rmgeovol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>All Remote Mirror Volumes</b> →(right-click a volume name)→ <b>Delete</b>
extendgeovol	Extending the size of a remotely mirrored volume	
	SMIT fastpath	<b>smit extendgeovol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>All Remote Mirror Volumes</b> →(right-click a volume name)→ <b>Extend</b>
replacegeovol	Replacing a disk within a remotely mirrored volume	
	SMIT fastpath	<b>smit replacegeovol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>All Remote Mirror Volumes</b> →(right-click a volume name)→ <b>Replace Disk</b>
volstat -X	Viewing I/O statistics for a remotely mirrored volume	
	SMIT fastpath	<b>smit statremotevol</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Volumes</b> → <b>All Remote Mirror Volumes</b> →(right-click a volume name)→ <b>Statistics</b>

## Remote Mirroring SMIT fastpaths and WebSM access

Table 38. Remote Mirroring SMIT fastpaths and WebSM access

Command	Description	
startmirror	Define a new NAS mirror.	
	SMIT fastpath	<b>smit startmirror</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>All Remote Mirror Devices</b> →(right-click a mirror device)→ <b>Start mirror</b>
stopmirror	Remove a NAS mirror.	
	SMIT fastpath	<b>smit stopmirror</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>All Remote Mirror Devices</b> →(right-click a mirror device)→ <b>Stop mirror</b>
startmirror	Start all mirrors.	
	SMIT fastpath	<b>smit startall</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>Overview and Tasks</b> → <b>Start all mirrors</b>
stopmirror	Stop all mirrors.	
	SMIT fastpath	<b>smit stopall</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>Overview and Tasks</b> → <b>Stop all mirrors</b>
geo_snapshot -t	Takes a snapshot of the mirror or mirrors.	
	SMIT fastpath	<b>smit geotake</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>Overview and Tasks</b> → <b>Create a snapshot of all remote mirroring devices</b>
geo_snapshot -a	Applies a snapshot of the mirror or mirrors.	
	SMIT fastpath	<b>smit geoapply</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>Overview and Tasks</b> → <b>Apply a snapshot of all remote mirroring devices to the system</b>
geo_snapshot -l	List snapshots of the remote mirroring devices	
	SMIT fastpath	<b>smit geolist</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Remote Mirroring</b> → <b>Overview and Tasks</b> → <b>List snapshots of remote mirror devices</b>

Table 38. Remote Mirroring SMIT fastpaths and WebSM access (continued)

Command	Description	
ismirror	List all remote mirroring devices	
	SMIT fastpath	<b>smit ismirror</b>
	WebSM	<b>NAS Management→NAS System→Remote Mirroring →All Remote Mirror Devices</b>
geonasviewlog	View Remote Mirroring logs.	
	SMIT fastpath	<b>smit log</b>
	WebSM	<b>NAS Management→NAS System→Remote Mirroring→Overview and Tasks→View Remote Mirroring logs</b>

## Snapshot SMIT fastpaths and WebSM access

Table 39. Snapshot SMIT fastpaths and WebSM access

Command	Description	
snapvol -C	Creates a snapshot.	
	SMIT fastpath	<b>smit snapvolC</b>
	WebSM	<b>NAS Management→NAS System→Snapshots Overview→Tasks→Create snapshot</b>
snapvol -Y	Configure a snapshot schedule.	
	SMIT fastpath	<b>smit snapvolY</b>
	WebSM	<b>NAS Management→NAS System→Snapshots Overview→Tasks→Configure a snapshot schedule</b>
snapvol -L	List snapshots.	
	SMIT fastpath	<b>smit snapvolL</b>
	WebSM	<b>NAS Management→NAS System→Snapshots→All Snapshots</b>
snapvol -N	Rename a snapshot.	
	SMIT fastpath	<b>smit snapvolN</b>
	WebSM	<b>NAS Management→NAS System→Snapshots Overview→Tasks→(right-click a snapshot)→Rename</b>
snapvol -r	Roll back a snapshot.	
	SMIT fastpath	<b>smit snapvolr</b>
	WebSM	<b>NAS Management→NAS System→Snapshots Overview→Tasks→(right-click a snapshot)→Rollback</b>
snapvol -R	Remove a snapshot.	
	SMIT fastpath	<b>smit snapvolR</b>
	WebSM	<b>NAS Management→NAS System→Snapshots Overview→Tasks→(right-click a snapshot)→Delete</b>

Table 39. Snapshot SMIT fastpaths and WebSM access (continued)

Command	Description	
snapvol -l	Show a snapshot schedule.	
	SMIT fastpath	<b>smit snapvoll</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Snapshots Overview</b> → <b>Tasks</b> →(right-click a snapshot)→ <b>Show Schedule</b>
snapvol -A	Activate a snapshot schedule.	
	SMIT fastpath	<b>smit snapvolA</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Snapshots Overview</b> → <b>Tasks</b> →(right-click a snapshot)→ <b>Activate Schedule</b>
snapvol -S	Stop a snapshot schedule.	
	SMIT fastpath	<b>smit snapvolS</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Snapshots Overview</b> → <b>Tasks</b> →(right-click a snapshot)→ <b>Stop Schedule</b>
snapvol -X	Delete a snapshot schedule.	
	SMIT fastpath	<b>smit snapvolX</b>
	WebSM	<b>NAS Management</b> → <b>NAS System</b> → <b>Snapshots Overview</b> → <b>Tasks</b> →(right-click a snapshot)→ <b>Delete Schedule</b>
snaplm	Creates and updates links for the desired volume.	
	SMIT fastpath	N/A
	WebSM	N/A
snaplmo	Disables snapshot link management for the desired volume.	
	SMIT fastpath	N/A
	WebSM	N/A
snaplmon	Choose settings for snapshot link management for the desired volume.	
	SMIT fastpath	N/A
	WebSM	N/A

---

## Appendix C. Remote Mirroring problem determination

The remotely mirrored volumes on the NAS Gateway 500 are examples of GeoMirror devices (GMDs). The mirroring network, which is the communication path between sites, is also called a GeoNetwork. Similarly, the two-site geographic cluster is referred to as a GeoCluster. This section discusses the various types of failures in a remote mirroring configuration and the steps required to recover that configuration. The following types of failures and recovery are discussed:

- Site failure (see “Site failure”)
- Site isolation (see “Site isolation” on page 296)
- Node failure (see “Node failure” on page 297)
- Disk failure (see “Disk failure” on page 297)
- Data divergence (see “Data divergence” on page 297)
- Catastrophic failures (see “Site recovery after catastrophic failure” on page 301)

---

### Site failure

Communication failures, scheduled and unscheduled kernel reboots, power failures and other short term failures that affect all the nodes at a site are considered to be site failures. When a site fails and then recovers, the NAS Gateway 500 automatically restarts the mirroring process to resynchronize the data on the recovering site. The cluster must then be manually started on that site to initiate a fallback of the resources.

**Note:** The cluster must not be started on the recovering site until the data synchronization is complete. If the cluster is started before data resynchronization is complete, that site’s resources are unavailable until the resynchronization completes.

If the GeoNetwork between the local and remote sites spans multiple subnets, IP address takeover will not allow client access to the file serving IP addresses. This occurs because those addresses will now reside on a different physical network link, but the network’s routers will not be aware of this and will continue to route traffic for those addresses to their old location. There are three ways to manage file serving IP addresses in case of a site failure:

- Use a single subnet for the GeoNetworks between the local and remote sites.
- When a site failure occurs, manually adjust network routers to route traffic for the file serving IP addresses to the new location.
- When a site failure occurs, modify clients to use a file serving IP address on the surviving site to access data.

### Handling site failures

Clustering, using Remote Mirroring tools, detects a site failure when no heartbeats are received on a Remote Mirroring network, including the secondary Remote Mirroring networks. Clustering sends appropriate warnings or messages to the cluster log at the surviving site.

To recover a failed site:

1. Monitor `nasxd.log` on the nodes at the recovering site. An entry will be logged indicating that synchronization is complete and the cluster may now be started.

2. When you are ready to initiate site failback, start the cluster on the recovering site from the command line (alternatively, you can use SMIT or WebSM from the Cluster Management menu). Either start the cluster on one node at a time with **Enable a Server in the Cluster** (the `clnasenode` command), or **Enable Cluster** (the `clnasencluster` command).
3. Failback of the recovering site resources is handled automatically by HACMP/XD. For more information, see “Reintegrating the failed site.”

### Reintegrating the failed site

Depending on the application, the surviving copy of the data might continue to change while the mirror copy is not available. The state map device is used to recover from these failures. When a failed site recovers and reintegrates, the state map is automatically processed to synchronize the data on the devices. The reintegration process proceeds as follows:

1. When the first remote node sends the message that it is ready to rejoin the cluster, Remote Mirroring on the functioning local site suspends the regular clustering reintegration process until the synchronization of the GeoMirror devices is complete. The nodes at the local site continue to process data while Remote Mirroring is bringing the remote node up to date.

**Note:** If the GeoMirror devices are already synchronized, this step does not apply.

2. When the remote node successfully rejoins the cluster, all the configured clustering applications become available immediately. After the first node is up, the site is functioning. The remaining nodes, those that participate in mirroring the devices that have already been synchronized once, rejoin at a faster rate. They do not have to wait for the synchronization process across the geography.
3. When nodes at a failed site reintegrate, the GeoMirror devices at both sites check the state map values for corresponding data regions to see if data needs to be transferred to the reintegrating device. The synchronization of the remote GeoMirror devices is a time-consuming process if extensive alterations to shared data occurred during the failure period. Synchronization must complete before the applications on the recovering site that use the GeoMirror device can be started. If the state maps on both sides of a device have cells marked stale, you must manually update the state map before the device can be started. See the section on data divergence to manually update the state map.
4. The HACMP™ Cluster Manager will process the `config_too_long` event as soon as the configuration time exceeds six minutes, which is highly likely for most instances of synchronization. This is not cause for alarm. The event causes the message to be displayed. The Cluster Manager continues the configuration process regardless of the messages.

---

## Site isolation

Site isolation occurs when all HAGEO networks are not available.

### Handling site isolation

The Cluster Manager might still be able to send heartbeats over a client network to realize that the remote nodes are functioning. The Cluster Manager, using the Remote Mirroring tools, recognizes that a `global_network_down` event has occurred and brings down the nondominant site to avoid data divergence as much as possible. When the Remote Mirroring networks are functioning again, the nondominant site can rejoin the cluster. The GeoMirror devices synchronize the

state map devices so that data at the rejoining site is brought up to date. If writes occurred on both sites during the site isolation situation, you must unify the state maps on the GeoMirror devices to correct any data divergence that occurred. Then you bring up the nodes at the rejoining site.

---

## Node failure

When a node at a site with more than one node fails, messages are logged to the system administrator. You should periodically check the logs as part of normal maintenance procedures. You can also have messages sent to the console. Clustering handles recovery from failures of local nodes, networks, and adapters. No GeoMirror synchronization is needed after the failure of a local peer, as long as the clustering failover succeeds or the configuration is concurrent. IP address takeover is not supported on Remote Mirroring networks.

---

## Disk failure

You can recover from failures such as the loss of a hard drive, which is not mirrored in the logical volume, using the **gmd\_update\_state** utility. Use this utility, for example, if a hard disk is replaced on a site. You can mark all the cells associated with the GeoMirror device logical volumes on the new hard disk as being stale. This causes the synchronization process to update the device from the peer device at the other site. We suggest that you implement LVM mirroring or use RAID techniques. It is possible that some I/O errors, when writing to GMDs, may cause inconsistencies that are not reflected in the GMD state map. Unrecoverable disk I/O errors are recorded in the AIX<sup>®</sup> error log. That log should be monitored to allow for controlled recovery in case these disk errors occur.

---

## Data divergence

**Attention:** Follow all instructions in this section with extreme care. If you **do not** follow instructions exactly, **loss of data is very likely**.

When the state maps for a GeoMirror device have cells that are marked stale in both sites, the GMDs cannot be started because the clustering manager cannot determine which data is most recently written. This data divergence occurs when the sites are not communicating, and information is written to the volumes at both sites without being mirrored to the other site. In order to recover the mirrored data the state maps must be unified. The following procedures explain the key points of the state maps and the unifying process.

## GeoMirror state map devices

The GeoMirror state map device is a key component in the process of recovery after various types of failures. Communication failures, power failures, and other short-term failures are considered site failures. Depending on the application, site failures can cause the surviving copy of the data to continue to change while the mirror copy is not available. When a site fails and recovers, the Remote Mirroring software synchronizes the GeoMirror device. It reads the appropriate state map for each node in order to reconstruct and update the mirror on the recovered node. This process of synchronizing the GeoMirror device is automatic. The intervention of the system administrator might be required in a failure such as the loss of a hard drive that is not mirrored in the logical volume.

**Note:** Be extremely careful if you modify a state map. Each node in the remote mirror configuration maintains, or shares, a state map for each of its

GeoMirror devices. Important transitions in the state of a data region, as it traverses the geographic mirroring process, are synchronously recorded in the state map. In that way, a GeoMirror device can be reconstructed based on the surviving copy and the associated state maps. The state map contains the current state of all data regions written on the GeoMirror device. The state map must be a unique logical volume. The state map is divided into cells that are four bits wide. By default, each cell represents one 32 KB data region of the GeoMirror device. A data region can be in any one of several states. The two key states are consistent and stale. The states are represented by hexadecimal values; 0x0 representing the consistent state, and 0x1–0xf representing the stale state.

## Viewing state map device information (root only)

To view the state map for a GeoMirror device issue, type the following:  
`/usr/sbin/gmd/gmd_show_state -l gmd`

where *gmd* is the name of the GeoMirror device. This can be either the GeoMirror device for the filesystems or the device for the JFS2 log device. To view the state map for all Geo Mirror devices issue, type: `/usr/sbin/gmd/gmd_show_state -A`

## Saving state maps in map files (root only)

It is possible to save a GeoMirror device state map in a map file. You can then view and manipulate the map file instead of the actual state map.

**Note:** These operations are available only on exceptional occasions. SMIT or WebSM windows are not available for these operations.

Operations allowed on a map file include:

- Dumping a state map to a map file
- Showing a map file
- Changing a map file (setting regions)
- Loading a map file on a given node.

**Note:** Loading a map file does not replace the current state map. Instead, the map file merges into the current state map.

## Updating a state map device (root only)

After replacing a failed hard disk, you can use the `gmd_update_state` utility to change a state map. You can set state cells in a state map to a specific value.

**Note:** Be extremely careful when attempting to modify a state map. A mistake can cause loss of data. To use the command line, see the section on "Updating a state map device" in the *High Availability Cluster Multi-Processing XD (Extended Distance) V5.1: Planning and Administration Guide for HAGEO Technology (SA22-7956-00)*.

To update a state map device using SMIT, do the following:

1. If a remote peer is active, stop the GeoMirror device.
2. Run the `smit hageo` fastpath command to open the main window.
3. Stop the GMDs.
4. Return to the GeoMirror Utilities window. Click **Change State Map** and press **Enter**. The following is displayed:



```

Change State Map

Move cursor to desired item and press Enter

Preview Unified State Map
Unify State State Maps
Set State in State Map

```

5. Click **Set State in State Map** and press **Enter**. A window similar to the following is displayed:

```

Set State in State Map

Type or select values in entry fields
Press Enter AFTER making all desired changes;

* Value                               [Entry Fields]
* Starting Data Region                Stale                +
Ending Data Region                    [ ]                  #
* Device Name                          [ ]                  #
Nonde name                             [ ]                  +

```

6. Make entries to set the entire state map to stale on the node where you need to update the disk, for example: GeoMirror device gmd0.

**Note:** Setting the whole state map to stale is the safest alternative in this situation. You have the option of setting a region less than the whole. But you must be certain not to make an error that could cause loss of data or data corruption. To set the entire state map to stale, use the entry fields as follows:

**Value** Enter **stale**. The other choice is consistent.

**Starting Data Region**  
Enter **0** to begin at the first region.

**Ending Data Region**  
Enter **-1** to cover all regions.

**Device name**  
In this example, enter **gmd0**.

**Node name**  
The default is the local node. If you are not doing the operation from the affected node, enter the node name of the affected node.

7. Press **Enter**.
8. Press **F3** to return to the GeoMirror Utilities window or **F10** to exit SMIT.

## Checking and unifying state maps

The procedure for checking and unifying state maps is outlined here. To check and unify state maps when at least one remote mirror network is available and GeoMessage is started on the local node, do the following:

1. View the state maps for GeoMirror devices on nodes at both sites. (See “Viewing state map device information (root only)” on page 298 for more information.) For example, running the **gmd\_show\_state** command for gmd0 (in mwc mode) on the local node clam might show output similar to the following:

```

Point of View: Node Clam
-----
Point of View GMD List:
-----
Name: gmd0
Status: AVAILABLE

State Map:
  Cell    Value
-----
  0       0x3 0x3 0x3 0xf 0xf 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
  16      0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

```

The result of the same command listing the state map for the same device on a remote peer node might be similar to the following:

```

State Map:
  Cell    Value
-----
  0       0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0xf 0xf 0xf 0xf
  16      0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

```

2. Note the cells that are different on the state maps for the device on the two nodes. The view point of the local and remote nodes in our example show different states for some cells in the same region. Since there are stale cells (writes) on both sides, the state maps must be manually unified.
3. From a local node at the available site, you can preview the result of unifying the state maps. The output shows what the unified state map should look like. For the example case, the preview of the unified state map is the following:

```

State Map:
  Cell    Value
-----
  0       0x3 0x3 0x3 0xf 0xf 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0xf 0xf 0xf 0xf
  16      0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

```

See “Previewing a unified state map” for additional information.

4. From a local node at the available site, you can unify the state maps for all GeoMirror devices and install them on the nodes at the active site. When communication between sites is restored, the GeoMirror devices on nodes at the rejoining site receive the unified state map information.

## Previewing a unified state map

To preview a unified state map using the **gmd\_show\_state** command with SMIT, do the following:

1. Run **smit hageo fastpath** to open the main window.
2. Click **HAGEO Utilities>GeoMirror Utilities** and press **Enter**.
3. When a remote peer is active, stop the GeoMirror device.
4. From the GeoMirror Utilities window, click **Change State Map**. Preview the Unified State Map and press **Enter**. A window similar to the following is displayed:

Preview Unified State Map

Type or select values in entry fields.  
Press Enter AFTER making all desired changes

\* Device name [Entry Fields]  
[] +

5. Enter the name of the device for which to show unified state map information. To see a list of devices to select, click on the Device Name option and press **F4**. The resulting output shows the unified state map, as illustrated in “Checking and unifying state maps” on page 299.

## Unifying state maps

The **gmd\_update\_state** utility sets state cells in the state map to a specific value or unifies all of the state maps for the specified GeoMirror device. To recover from site isolation, you need to shut down one site. Then you can unify all the state maps for all GeoMirror devices on the active site.

**Note:** You can set state cells in the state map to a specific value, but you must be extremely careful if you attempt to modify a state map. A mistake can cause loss of data or data corruption.

For more information on unifying state maps, refer to the section on “Updating a state map device” in the *High Availability Cluster Multi-Processing XD (Extended Distance) V5.1: Planning and Administration Guide for HAGEO Technology (SA22-7956-00)*.

## Site recovery after catastrophic failure

Remote Mirroring is intended to provide timely access to mission-critical data in the event of a disaster that destroys or disables an entire site location. Problems can range from an electrical failure involving the entire site to the entire site being permanently disabled by fire, flood, or an earthquake. Remote Mirroring enables the restoration of computing services even if all of the hardware must be replaced. If you must completely replace the hardware and software at a site, or replace a destroyed site by locating its components in another geographic area, you need up-to-date copies of the planning worksheets so you can configure the site according to its state at the time of the disaster. Since there will probably be a great deal of data to synchronize, the integration process might take a long time. The time it takes to synchronize depends on several factors:

- Amount of data changed since the outage: More data increases the time needed
- Number of GeoMirror devices involved in the process: More mirrors increase the time needed
- Size of the GeoMirror devices: Bigger mirrors increase the time needed
- Network bandwidth available: Lower bandwidth increases the time needed
- Network traffic: High traffic increases the time needed



---

## Appendix D. Cluster snapshot configuration

The NAS Gateway 500 allows you to save information used to configure the cluster in a cluster snapshot. A cluster snapshot is a useful tool for disaster recovery because it allows a node to restore its configuration in the event that the node experiences a failure that corrupts its configuration. It can also be useful for problem determination because the snapshot is saved in two text files that can easily be retrieved and used to show the current cluster configuration.

Cluster snapshot configuration is also supported in a remote mirroring cluster. The only difference is that to apply a snapshot in a remote mirroring cluster, the cluster must be stopped so that it can be synchronized.

**Note:** If a node containing a cluster snapshot has its operating system removed (such as the case when the node is re-imaged), the cluster snapshot will no longer be available. The stored information will have been removed and a new cluster snapshot will need to be created for any future system restorations with a cluster snapshot.

The following tasks are available when configuring and using a cluster snapshot:

- “Adding a cluster snapshot”
- “Changing and showing a cluster snapshot” on page 304
- “Removing a cluster snapshot” on page 304
- “Applying a cluster snapshot” on page 304
- “Configuring a custom snapshot method” on page 305

---

### Adding a cluster snapshot

Adding a cluster snapshot will store the necessary information to configure the cluster on a node. Cluster snapshot management is part of HACMP. To add a cluster snapshot, you must use the **smit hacmp** fastpath.

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Add a Cluster Snapshot** and press **Enter**.
5. Enter the name you want to call the snapshot and a description of the snapshot. If you want to save the logs for the cluster, highlight that field and press **Esc+4**, and then select **yes**.
6. You can also optionally select **Custom Defined Snapshot Methods**. To use a custom method, highlight the Custom Defined Snapshot Methods field and press **Esc+4**. To select one or multiple custom methods press **Esc+7**. If you want to use all custom defined methods, select **All** at the bottom with **Esc+7**.

**Note:** See “Configuring a custom snapshot method” on page 305.

7. Press **Enter** after entering the name, description, and the optional custom snapshot method information. This will create the cluster snapshot on all nodes in the cluster. A confirmation dialog asking **ARE YOU SURE?** is displayed. Press **Enter** to continue the creation or press **Esc+3** to cancel.
8. The Command Status is displayed when creating the snapshot. The Command: field shows OK when the command finishes execution.
9. Press **Esc+0** to exit SMIT after the command process finishes.

---

## Changing and showing a cluster snapshot

Changing a cluster snapshot allows you to alter the name of the snapshot and the description of the snapshot. You can also optionally show the same information without changing the snapshot.

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Change/Show a Cluster Snapshot** and press **Enter**. A list of available cluster snapshots is displayed. Select the snapshot you want to change or show and press enter.
5. The snapshot information regarding the name and description of the snapshot is displayed. If you only want to show the information, then press **Esc+0** to exit SMIT.
6. If you want to change the name of the snapshot, enter the new name in the New Cluster Snapshot Name field.
7. If you want to change the description of the snapshot, enter the new description in the Cluster Snapshot Description field.
8. Press **Enter** after making all desired changes to save the new cluster snapshot information. A confirmation dialog asking ARE YOU SURE? is displayed. Press **Enter** to continue or press **Esc+3** to cancel.
9. The Command Status is displayed while the change is occurring. The Command: field shows OK when the command finishes execution.
10. Press **Esc+0** to exit SMIT when the process finishes execution.

---

## Removing a cluster snapshot

If you have a snapshot that you no longer want to keep, that snapshot can be removed.

**Note:** Removing the snapshot does not remove the current cluster configuration. However, removing the snapshot does remove the snapshot on all nodes in the cluster.

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Remove a Cluster Snapshot** and press **Enter**.
5. A list of available snapshots that can be removed is displayed. Select the snapshot you want to remove and press **Enter**. A confirmation dialog asking ARE YOU SURE? is displayed. Press **Enter** to continue or press **Esc+3** to cancel.
6. The Command Status is displayed during the removal. The Command: field shows OK when the command finishes execution.
7. Press **Esc+0** to exit SMIT when the process completes.

---

## Applying a cluster snapshot

If you have an existing cluster snapshot, then you can use that snapshot at anytime to reconfigure the cluster. The snapshot can be used to reset the cluster to an earlier state and remove configuration changes made after the snapshot was created. A snapshot can also be unconfigured so that changes made as a result of

applying the snapshot are removed and an automatically saved snapshot (at the time the first one was applied) can be used to restore the previous cluster configuration.

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Apply a Cluster Snapshot** and press **Enter**. A list of available snapshots is displayed. Select the snapshot you want and press **Enter**.

**Note:** All automatically saved snapshots are also displayed. They are listed as ~snapshot.n where n is 1, 2, or 3. If you are unconfiguring a previously applied cluster snapshot, select one of these snapshots where 1 is the saved configuration from the most recently applied cluster snapshot.

5. The snapshot name and description are displayed. Press **Esc+4** and select **Yes** or **No** for the Un/Configure Cluster Resources? field.

If you select **Yes**, then HACMP changes the definition of the resource in the Configuration Database and it performs any configuration triggered by the resource change. For example, if you remove a filesystem, HACMP removes the filesystem from the Configuration Database and also unmounts the filesystem.

If you select **No**, then HACMP changes the definition of the resource in the Configuration Database but does not perform any configuration processing that the change may require. For example, a filesystem would be removed from the HACMP cluster definition but would not be unmounted.

6. If you want the snapshot to be applied if verification fails, select **Force apply if verify fails?**, press **Esc+4** and then select **Yes** or **No**. Verification is performed to check to new configuration. If verification fails, synchronization is aborted. This will normally stop the new snapshot from being applied. Selecting **Yes** for this field applies the new snapshot even if verification fails.
7. Press **Enter** after making your selections to start the process of applying the new snapshot. A confirmation dialog asking ARE YOU SURE? is displayed. Press **Enter** to continue or press **Esc+3** to cancel.

**Note:** If you are running a remote mirroring cluster, you must first stop the cluster in order for it to be synchronized. Synchronization is necessary so that all nodes in the remote mirroring cluster have updated configuration information.

8. The Command Status is displayed during the removal. The Command: field shows OK when the command finishes execution.

**Note:** During the command execution, the current configuration is automatically saved as ~snapshot.1. Any previously automatically-saved configurations increment (a previous ~snapshot.1 will now become ~snapshot.2, and so on). A maximum of three automatic snapshots are saved.

9. Press **Esc+0** to exit SMIT when the process finishes execution.

---

## Configuring a custom snapshot method

A default cluster snapshot saves only HACMP Configuration Database classes information and the present state of the cluster directly related to HACMP. You can optionally save the logs with the cluster snapshot; however, all other information is not maintained in a cluster snapshot. If you want to save additional information with

your cluster snapshot, you can configure a custom snapshot method. Three tasks are available for configuring a custom snapshot method:

- “Adding a custom snapshot method”
- “Changing or showing a custom snapshot method”
- “Removing a custom snapshot method”

## Adding a custom snapshot method

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Configure Custom Snapshot Method**.
5. To add a custom snapshot method, select **Add a Custom Snapshot Method** and press **Enter**.
6. Enter the name of the custom snapshot and any description of it in the corresponding fields. For the Custom Snapshot Script Filename, enter the path of the script you want to use with your cluster snapshot.

**Note:** This script is a user defined script that is used to store information.

7. Press **Enter** and the custom method is saved.
8. Press **Esc+0** to exit SMIT

## Changing or showing a custom snapshot method

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Configure Custom Snapshot Method**.
5. To change or show a custom snapshot method, select **Change/Show a Custom Snapshot Method** and press **Enter**. A list of available custom methods is displayed. Select the method you want to change.
6. The custom snapshot information is displayed. If you only want to show the custom method information, press **Esc+0** to exit SMIT.
7. You can change the New Custom Snapshot Method Name, Custom Snapshot Method Description, and Custom Snapshot Script Filename fields used for the custom method. Select the fields you want to change and enter the new values.
8. Press **Enter** and the custom method is changed.
9. Press **Esc+0** to exit SMIT.

## Removing a custom snapshot method

1. Enter the **smit hacmp** fastpath.
2. Select **Extended Configuration** and press **Enter**.
3. Select **Snapshot Configuration** and press **Enter**.
4. Select **Configure Custom Snapshot Method**.
5. To remove a custom snapshot method, select **Remove a Custom Snapshot Method**.
6. A list of available methods to be removed is displayed. Select the method you want to remove and press **Enter**. A confirmation dialog asking ARE YOU SURE? will be displayed. Press **Enter** to continue the removal or press **Esc+3** to cancel.



7. The custom method is removed. Press **Esc+0** to exit SMIT.



---

## Appendix E. Hardware installation and service updates

**Note:** Serial port 1 is reserved for the management console. The tty port must have login enable set to *enabled*. For more information on console strategy, refer to the *IBM TotalStorage NAS Gateway 500 Service Guide*.

Some general changes to the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide* and the *IBM TotalStorage NAS Gateway 500 Service Guide* are:

- References to *Cluster system* now include both the local and remote site nodes.
- When Clustering is purchased with Remote Mirroring, a single site can contain a maximum of two nodes and a single cluster can contain a maximum of two sites.
- When Clustering is purchased without Remote Mirroring, it can contain a maximum of one site with two nodes.
- Even when the Remote Mirroring cluster contains only one node at a site, the restrictions associated with Clustering still apply to that node. For example, never run the default **root cfgmgr**, since it is a part of the larger cluster. Always use the `/opt/nas/bin/cfgmgr` command.
- The 4GB memory Feature Code 4453 is withdrawn and is replaced by FC 4490.
- Before replacing any FRU, check the support Web site for new or updated firmware for both the system and the devices (such as adapters).
- Call Home is no longer provided by the Service Processor. Call Home is now provided through IP as well as modem by the Electronic Service Agent software.
- Appendix B, in the *IBM TotalStorage NAS Gateway 500 Service Guide* is replaced by Appendix A in this guide.

---

### Stopping the system

**Note:** This information replaces that described in the *IBM TotalStorage NAS Gateway 500 Service Guide* and the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*.

**Attention:** When shutting down your system to perform service or install options, shut down all applications first and then shut down the operating system. The system power turns off and the system goes into standby mode when the operating system is shut down and OK is displayed on the op panel. Before removing power from the system, ensure that the shutdown process is complete. Failure to do so can result in the loss of data.

Some option-installation and service procedures do not require the system to be stopped for installation. The option-installation and service procedures in the *Hardware Installation Guide* and *Service Guide* will indicate if this procedure is required.

1. If the operator panel displays the **OK** prompt, go to step 8 on page 310.
2. Log in to the system as *root*.
3. Have your system administrator stop all applications that are running on the system. If you are not clustering, go to step 7 on page 310. If you are clustering, continue with step 4.
4. If clustering, you need to relocate this node's volumes over to the other cluster node.
  - a. To display the hostname of this node, enter `hostname` on the command line.

- b. To display the hostname of the local site peer node, enter `/opt/nas/lib/cluster/clnaspeer -n hostname` .
- c. If there is no local peer node, display the name of the remote site node or nodes by entering `/opt/nas/lib/cluster/geonasremotenodes -n <this hostname>`. The first name listed is the primary node at the remote site.

**Note:** Record all the hostnames.

5. To display the group name or names of the volumes being served on this node, enter `/opt/nas/bin/clnasshowvol -a -n <this hostname>`.

**Note:** Record all group names.

6. Stop the cluster on the node being serviced. Force a failover by entering `/opt/nas/bin/clnasdisnode -n <this hostname> -f`. Failover is then forced to the local site peer node if there is one in the cluster; otherwise, it is forced to the remote site primary node. In the remote-only case, only remotely mirrored volumes are failed over. All other (non-remotely mirrored) volumes will not be accessible while this node is powered down.
7. At a command line, enter `shutdown` to stop the operating system. If you cannot use this method, power off the system by pressing the operator panel power button.

**Attention:** Using the operator panel power button to power off the system can cause unpredictable results, and the next IPL will take longer to complete. It will also cause the attention LED to light the next time.

8. After you shut down the operating system (operator panel displays the OK prompt), set the power switches of any attached devices to Off.
9. If necessary, disconnect the power sources to both the NAS Gateway 500 power supplies.

---

## Restarting the system

To power on the system, perform the following steps:

1. If both power sources were disconnected, reconnect them to the system.
2. Before you press the power button on your operator panel (Figure 54 on page 311), ensure that:
  - The power LED is slowly blinking.
  - An OK prompt is visible in the operator panel.
3. Press the power-on button on the operator panel. After pressing the power button located on the operator panel, ensure that:
  - The power LED begins to blink faster.
  - The system cooling fans are activated and begin to accelerate up to operating speed.

**Note:** There is a transition period of approximately 40 seconds between the time the power button is pressed and the power LED remains solid (no longer blinking).

- The power LED stays solid and the progress indicators (also referred to as *checkpoints*) are visible on the operator panel.

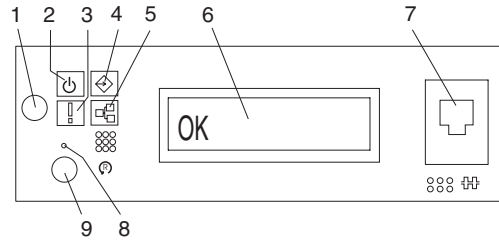


Figure 54. Operator panel

- 1 Power-on button
- 2 Power-on LED (blinks when in standby)
- 3 Attention LED
- 4 SCSI port activity LED
- 5 Ethernet port activity LED
- 6 Operator panel display
- 7 RJ-48 front serial port 1 connector (serial port 1)
- 8 Service processor reset switch (pinhole)
- 9 System reset button

**Note:** The boot process can take 15-30 minutes, depending on the system configuration and attachments. Approximately 30 seconds after the boot process has completed, the operator panel will go blank (unless this is the very first boot before initial configuration is complete; then the IP address for Ethernet port 1 is displayed). At this point, you can ping or telnet into the machine. If a console is attached to serial port 1, the POST messages and checkpoints are displayed on the console, and, when boot is complete, the login prompt displays. Messages might continue to display after the login prompt.

4. If this node was clustered previously, bring this node back into the cluster pair to resume file serving using the hostname and group name or names recorded prior to shutdown:
  - a. Log in to the system as *root*.
  - b. At the command line, rejoin the cluster by entering `opt/nas/bin/clnasenode -n <this hostname>`.
  - c. Poll status until the node has finished stabilizing: `opt/nas/bin/clnasnodestate -n <this hostname>`.
  - d. Once the status changes to *stable*, the volumes should be relocated back to this node for file serving. This happens automatically if failover was forced to the remote site primary node, or if Auto Failback was selected when the local site cluster nodes were configured. If AutoFail was not selected on the local site, then you must manually relocate the volumes back to this node by entering `/opt/nas/bin/clnasrelocate -g <groupname> -n <this hostname>` for all group names.

---

## Installing the OS mirroring option

You do not need to power off the system to add a hot-plug disk drive. Before you perform these procedures, ensure that you have taken appropriate actions to back up the data for the drive that you are mirroring.

**Note:** This information replaces that described in the *IBM TotalStorage NAS Gateway 500 Hardware Installation Guide*.

To install a hot-plug disk drive, perform the following steps:

1. Remove the front bezel, as described in the *Hardware Installation Guide*.
2. Remove the disk drive from its protective packaging, and open the drive latch handle.
3. Install the disk drive in the drive slot. Align the disk drive with the drive slot rails, and slide the disk drive into the slot until it contacts the backplane at the rear of the drive bay. The drive should be in far enough for the latch handle to engage the latch. Push the disk drive lever up and to the rear to secure the disk drive. The LED on the disk drive will turn on and start to blink.
4. Log into the machine as *root*.
5. After the HDD LED has stopped blinking, enter `/opt/nas/bin/cfgmgr` on the command line. This configures the hard drive and makes the hard drive available for operations.
6. At the command line, enter `lspv`. A list appears with the available hdisks.
7. Record the first available local hdisk after `rootvg`. This hdisk is used at a later time in this procedure. At the command line, enter `smit extendvg`.
8. Enter the following code for each empty section:
  - a. When asked *Force the creation of volume group?*, use the Tab key to select YES.
  - b. In the volume group name section, enter `rootvg`.
  - c. In the physical volume name section, enter the name of the hdisk from step 7 and press **Enter**.
9. Once the command completes, press **Esc + 0** and at the command line, enter `smit vg`.
10. Select **Mirror a Volume Group** and press **Enter**.
11. In the volume group name section, enter `rootvg`.
12. In the physical volume name section, enter the name of the hdisk from step 7 and press **Enter**.
13. When you have finished, press **Esc + 0** to exit SMIT.
14. At the command line, enter `bosboot -a`. This command checks to see if you are able to boot from both drives.
15. At the command line, enter `bootlist -m normal hdisk0 <hdisk#>`. This institutes the proper boot order.

**Note:** `hdisk#` is the name of the hdisk from step 7.

16. To verify a successful mirror, enter `lsvg rootvg` at the command line.
17. Verify that the active PV number is 2.
18. Replace the bezel as described in the *Hardware Installation Guide*.

---

## Appendix F. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

---

## Trademarks

IBM, the IBM logo, ServeRAID, DB2, ServerGuide, TotalStorage, NetView, SecureWay, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Alacritech and SLIC Technology are registered trademarks of Alacritech, Inc. in the United States, other countries, or both.

Intel, LANDesk, MMX, Pentium, Pentium II Xeon, Itanium, and Pentium III Xeon are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Lotus and Domino are trademarks of Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

NetWare is a trademark of Novell, Inc.

Persistent Storage Manager is a trademark of Columbia Data Products, Inc.

UNIX is a registered trademark in the United States, other countries, or both, and is licensed exclusively through X/Open Company Ltd.

Other company, product, and service names may be trademarks or service marks of others.



---

# Glossary

---

## Glossary of terms

This glossary defines technical terms and abbreviations that this book uses. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at:

[www.ibm.com/networking/nsg/nsgmain.htm](http://www.ibm.com/networking/nsg/nsgmain.htm)

This glossary also includes terms and definitions from:

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). You can purchase copies from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms*. New York: McGraw-Hill, 1994.

This glossary uses the following cross-reference convention:

**See** Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

**See also**  
Refers you to a related term.

## Numerics

**10BASE-T.** The IEEE 802.3 Ethernet standard that supports a transmission rate of 10 Mbps using two twisted-pair wires (Category 3 telephone wiring).

**100BASE-T.** The IEEE 802.3 Ethernet standard that supports a transmission rate of 100 Mbps using two twisted-pair wires (Category 5 telephone wiring).

## A

**access control.** In computer security, the process of ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.

**access control list (ACL).** (1) A collection of all access rights for one object. (2) A list associated with an object that identifies all the subjects that can access the object and their access rights; for example, a list associated with a file might identify users who can access the file and their access rights to that file.

**accessory.** An IBM designation for a separately orderable part that (a) has no type number, (b) is for purchase only, and (c) does not receive normal IBM maintenance.

**ACL.** See *access control list*.

**adapter load balancing.** The ability of several adapters in a team to be active simultaneously, with the outbound-traffic load balanced across all the adapters in the team; spreading tasks among adapters improves performance by preventing uneven distribution of workload. If one adapter in the team fails, the outbound traffic is redistributed across the remaining active adapters in the team. See also *teaming*.

**assigned disk.** A disk that is mapped to a logical drive.

**asynchronous.** A class of data-transmission service whereby all requests for service contend for a pool of dynamically allocated ring bandwidth and response time.

**attach.** To make a device a part of a network logically. Contrast with *connect*.

**attachment.** A port or a pair of ports, optionally including an associated optical bypass, that are managed as a functional unit. A dual attachment includes two ports: a port A and a port B. A single attachment consists of one port: port S.

**attention (ATTN).** An occurrence external to an operation that could cause an interruption of the operation.

**ATTN.** See *attention*.

## B

**bandwidth.** The capacity of a communications line or processor, normally expressed in bits per second (bps) or transactions per seconds (tps).

**baseband LAN.** A local area network in which data is encoded and transmitted without modulation of a carrier (T).

**Basic Input/Output System (BIOS).** The personal computer code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

**BIOS.** See *Basic Input/Output System*.

**bits per second (bps).** The rate at which bits are transmitted per second. Contrast with *baud*.

**boot IP address.** The IP address on which an Ethernet adapter boots prior to being assigned a service IP address.

**bps.** See *bits per second*.

**buffer.** See *buffer storage*.

**buffer storage.** (1) A special-purpose storage or storage area allowing, through temporary storage, the data transfer between two functional units having different transfer characteristics. A buffer storage is used between non-synchronized devices, a serial and a parallel device, or between devices having different transfer rates. (2) In word processing, a temporary storage in which text is held for processing or communication (T).

**bus.** See *data bus*.

## C

**cache.** A high-speed buffer storage that contains frequently accessed instructions and data to reduce access time.

**carrier sense multiple access with collision detection (CSMA/CD).** A class of medium access procedures that allows multiple stations to access the medium at will, without explicit prior coordination, and avoids contention by way of carrier sense and deference. Contention is resolved by way of collision detection and transmission.

**cascade.** To connect in a series or in a succession of stages so that each stage derives from or acts upon the product of the preceding stage.

**cascading resource group.** A resource group in which takeover priority is assigned to each configured node in the cluster such that ownership preferences is given to the highest priority node. Cascading resource groups exist only on one node at a time.

**CIFS.** See *Common Internet File System*.

**client.** A computer system or process that requests access to the data, services, or resources of a server (another computer system or process). Multiple clients may share access to a common server.

**client/server model.** A common software model in which a server program waits for requests from client programs and responds when a request is received. Requests and responses can be sent over a network if the client and server programs are running on different systems. An example is a HTTP server and web browser. When a web browser (client) sends a request for a web page, the HTTP server receives the request and responds by sending the requested web page back to the web browser.

**cluster.** In high-availability cluster multiprocessing (HACMP), a set of independent systems (called nodes) that are organized into a network for the purpose of sharing resources and providing failover capabilities in case a node fails. NAS Gateway 500 systems can be clustered to create highly-available systems that continue to be available if one node experiences a failure. See also *high-availability cluster multiprocessing (HACMP)* and *geographic cluster*.

**collision avoidance.** In carrier sense multiple access with collision avoidance (CSMA/CA), the process of sending a jam signal and waiting for a variable time before transmitting data. The process is designed to avoid two or more simultaneous transmissions.

**Common Internet File System (CIFS).** A protocol that enables collaboration on the Internet by defining a remote file-access protocol that is compatible with the way applications already share data on local disks and network file servers.

**communications protocol.** In networking, a set of standards defining how computers are to exchange information.

**connect.** In a LAN, to physically join a cable from a station to an access unit or network connection point. Contrast with *attach*.

**control unit.** A processor electronics assembly in a storage controller that exposes logical unit numbers (LUNs) to the storage network and connects internally to the storage controller's disk drives. A storage controller can have 1 to  $n$  control units, but typically has one for each path group. See also *logical unit number (LUN)*.

**CRC.** See *cyclic redundancy check*.

**CRU.** See *customer-replaceable unit*.

**customer-replaceable unit (CRU).** An assembly or part that a customer can replace in its entirety when any of its components fail. Contrast with *field-replaceable unit*.

**cyclic redundancy check (CRC).** (1) A redundancy check in which the check key is generated by a cyclic algorithm (T). (2) A system of error checking performed at both the sending and receiving station after a block-check character has been accumulated.

## D

**DASD.** See *direct access storage device*.

**data bus.** A bus used to communicate data internally and externally to and from a processing unit, storage, and peripheral devices (A).

**device identifier (ID).** An 8-bit identifier that uniquely identifies a physical I/O device.

**device parity protection.** A function that protects data stored on a disk-unit subsystem from being lost because of the failure of a single-disk unit in the disk-unit subsystem. When a disk-unit subsystem has device parity protection and one of the disk units in the subsystem fails, the subsystem continues to run. The disk-unit subsystem reconstructs the data after the disk unit in the subsystem is repaired or replaced. See also *RAID*.

**DHCP.** See *Dynamic Host Configuration Protocol*.

**DIMM.** See *dual inline memory module*.

**direct access storage device (DASD).** A mass-storage medium on which a computer stores data. Contrast with *random access memory (RAM)*.

**Direct Memory Access (DMA).** A technique in which an adapter bypasses a computer's CPU, and performs the transfer of data between itself and the system's memory directly.

**DMA.** See *Direct Memory Access*.

**DNS.** See *Domain Name System*.

**Domain Name System (DNS).** In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

**dominant site.** The site that will take over in case all communication is lost between sites.

**drive bay.** A receptacle in the NAS Gateway 500 into which you insert a hard-disk-drive module. The bays are in storage units that can be located in a different rack from the NAS Gateway 500.

**dual inline memory module (DIMM).** A small circuit board with memory-integrated circuits containing signal and power pins on both sides of the board.

**Dynamic Host Configuration Protocol (DHCP).** A protocol defined by the Internet Engineering Task Force (IETF) that is used for dynamically assigning IP addresses to computers in a network.

## E

**EIA.** See *Electronic Industries Association*.

**EISA.** See *Extended Industry Standard Architecture*.

**electromagnetic compatibility (EMC).** The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate correctly in the intended electromagnetic environment.

**Electronic Industries Association (EIA).** An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

**Electronic Industries Association (EIA) unit.** A unit of measure equal to 4.45 cm (1.75 in.).

**electrostatic discharge (ESD).** An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

**EMC.** See *electromagnetic compatibility*.

**engine.** The unit that contains the processors that respond to requests for data from clients. The operating software for the NAS Gateway 500 resides in the engine.

**equivalent paths.** A collection of paths to the storage device. The paths have no switchover time penalty when changing from one path group to another while accessing the storage device.

**error.** A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition (A) (I). Contrast with *failure*.

**ESD.** See *electrostatic discharge*.

**ESM.** See *environmental service monitor*.

**Ethernet.** A standard protocol for a 10-Mbps baseband local area network (LAN) that allows multiple access and manages contention by using carrier sense multiple access with collision detection (CSMA/CD) as the access method.

**Ethernet network.** A baseband LAN with a bus topology in which messages are broadcast on a coaxial cable using a carrier sense multiple access/collision detection (CSMA/CD) transmission method.

**expansion slot.** In personal-computer systems, one of several receptacles in the rear panel of the system unit into which a user can install an adapter.

**Extended Industry Standard Architecture (EISA).** The PC bus standard that extends the AT bus (ISA bus) to 32 bits and provides support for bus master. It was announced in 1988 as a 32-bit alternative to the Micro Channel that would preserve investment in existing boards. PC and AT cards (ISA cards) can plug into an EISA bus.

## F

**fabric.** A complex network using hubs, switches and gateways. For example, Fibre Channel uses a fabric to connect devices. A fabric can be as simple as a single cable connecting two devices.

**failback.** The restoration of the NAS Gateway 500 to its initial configuration after detection and repair of a failed network or component.

**failover.** (1) The automatic recovery of resources in the event of a network outage, or failure of the hardware or software. (2) A cluster event in which the primary database server or application server switches to a backup system due to the failure of the primary server.

**failure.** (1) The termination of the ability of a functional unit to perform its required function. (2) An uncorrected hardware error. Failures are either recoverable or not recoverable by the software or the operator. The operator is always notified when failures occur. Contrast with *error*.

**failover.** Also called failover. The process of an active node acquiring resources previously owned by another node, in order to maintain availability of those resources.

**fallback.** Also called failback. Process of a joining or reintegrating node acquiring resources previously owned by another node.

**Fast Etherchannel (FEC).** A proprietary technology developed by Cisco that creates a team of two to four 10/100 Ethernet adapters or ports to increase transmission and reception throughput. Adapter fault tolerance is also supported by this technology.

**Fast Ethernet.** An Ethernet standard that provides a data rate of 100 Mbps.

**feature code.** A code used by IBM to process hardware and software orders.

**FEC.** See *Fast Etherchannel*.

**Federal Communications Commission (FCC).** A board of commissioners appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign communications by wire and radio originating in the United States.

**fiber optic cable.** See *optical cable*.

**field-replaceable unit (FRU).** An assembly that is replaced in its entirety when any one of its components fails. In some cases, a FRU may contain other FRUs. Contrast with *customer-replaceable unit*.

**File Transfer Protocol (FTP).** In the Internet suite of protocols, an application layer protocol that uses TCP/IP and Telnet services to transfer bulk-data files between machines or hosts.

**flash memory.** A type of non-volatile storage device that must be erased in fixed blocks rather than single bytes.

**FRU.** See *field-replaceable unit*.

**FTP.** See *File Transfer Protocol*.

## G

**gateway.** A device that acts as a router to transfer packets between networks, but occurs at the transport layer. See also *router*.

**GB.** see *gigabyte*.

**GBIC.** See *Gigabit Interface Converter*.

**GEC.** See *Gigabit Etherchannel*.

**geographic cluster (GeoCluster).** A cluster with remote mirroring. A highly available system consisting of two sites that can be geographically distant from one another. This allows for continued availability in the case of the failure of an entire site. Each site can contain one or two nodes, for a total of up to four nodes in the geographic cluster. The sites communicate with each other over GeoNetworks. See also *cluster*, *HACMP/XD*, and *GeoNetwork*.

**GeoNetwork.** Ethernet path by which data is mirrored between the local and remote sites of a *GeoCluster*.

**GHz.** see *gigahertz*.

**gigabyte (GB).** In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

**Gigabit Etherchannel (GEC).** A proprietary technology developed by Cisco that creates a team of two Gigabit Ethernet adapters to increase transmission and reception throughput. Adapter fault tolerance is also supported by this technology.

**Gigabit Interface Converter (GBIC).** An encoding/decoding device that is a Class-1 laser component assembly with transmitting and receiving receptacles that connect to fiber-optic cables.

**gigahertz (GHz).** A unit of measure of frequency. One gigahertz equals 1 000 000 000 hertz.

**GMD.** GeoMirror devices (for example, remotely mirrored volumes).

## H

**HACMP.** see *high availability cluster multiprocessing*.

**high availability cluster multiprocessing (HACMP).** An AIX Licensed Program Product (LPP) that provides clustering function. An HACMP cluster can include up to 32 nodes.

**HACMP/XD.** see *high availability cluster multiprocessing extended distance*.

**high availability cluster multiprocessing/extended distance (HACMP/XD).** An AIX Licensed Program Product (LPP) that provides the capability for mirroring data across TCP/IP point-to-point networks over an unlimited distance from one geographic site to another.

**heartbeat.** Also called Keepalive. State-of-health message exchanged between nodes. Means of detecting failure in a cluster.

**high availability.** A model for maintaining computer service availability. It views service availability not as a series of replicated physical components, but rather as a set of system-wide, shared resources that cooperate to guarantee essential services.

**hertz (Hz).** A unit of frequency equal to one cycle per second.

**Note:** In the United States, line frequency is 60 Hz or a change in voltage polarity 120 times per second; in Europe, line frequency is 50 Hz or a change in voltage polarity 100 times per second.

**host.** (1) In TCP/IP, any system that has at least one Internet address associated with it. A host with multiple network interfaces may have multiple Internet addresses associated with it. The host can be a client, a server, or both. (2) In fibre-channel technology, any system that has at least one worldwide name associated with it. A host with multiple network interfaces may have multiple worldwide names associated with it.

**host processor.** See *host computer*.

## I

**IDE.** see *integrated development environment*.

**integrated development environment (IDE).** A set of software development tools such as source editors, compilers, and debuggers, that are accessible from a single user interface.

**IETF.** See *Internet Engineering Task Force*.

**iLUN.** See *iSCSI client logical-unit number*.

**IML.** See *initial microcode load*.

**integrated development environment (IDE).**

**IP aliasing, IP address takeover (IPAT) through IP aliasing.** A networking capability that allows placing a service IP address into a network interface as an alias, and keeping the old (boot) IP and hardware address.

**initial microcode load (IML).** The process of loading the operational microcode.

**interference.** (1) The prevention of clear reception of broadcast signals. (2) The distorted portion of a received signal. (3) In optics, the interaction of two or more beams of coherent or partially coherent light.

**Internet Engineering Task Force (IETF).** The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet. The IETF consists of numerous working groups, each focused on a particular problem. Internet standards are typically developed or reviewed by individual working groups before they can become standards.

**Internet Protocol (IP).** A protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network.

**interrupt request (IRQ).** An input found on a processor that causes it to suspend normal instruction execution temporarily and to start executing an interrupt handler routine.

**IP.** See *Internet Protocol*.

**IRQ.** See *interrupt request*.

**iSCSI client logical-unit number (iLUN).** A unique number that is assigned to each virtual logical unit number (VLUN). The iLUN for a single client starts at zero and increments sequentially.

## J

**JBOD.** Just a bunch of disks.

**JBON.** Just a bunch of nodes.

**jumper.** A connector between two pins on a network adapter that enables or disables an adapter option, feature, or parameter value.

**jumper cable.** See *patch cable*.

## L

**LAN.** See *local area network*.

**LIP.** See *loop initialization process*.

**local area network (LAN).** A network in which a set of devices is connected to one another for communication and that can be connected to a larger network.

**logical drive.** A unit of virtual storage that is made available to the network through virtual logical unit numbers (VLUNs) and iSCSI client logical-unit number (iLUNs). It consists of one or more physical disks that are combined using RAID 0, 1, 1E, 5, or 5E technology.

**logical partition (LPAR).** A fixed-size portion of a logical volume. A logical partition is the same size as the physical partitions in its volume group. Unless the logical volume of which it is a part is mirrored, each logical partition corresponds to, and its contents are stored on, a single physical partition.

**logical unit.** A type of network-accessible unit that enables users to gain access to network resources and communicate with each other.

**logical unit number (LUN).** An identifier used on a SCSI bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

**loop.** A closed unidirectional signal path connecting input/output devices to a system.

**LUN.** See *logical unit number*.

## M

**management information base (MIB).** Simple Network Management Protocol (SNMP) units of managed information that specifically describe an aspect of a system, such as the system name, hardware number, or communications configuration. A collection of related MIB objects is defined as a MIB.

**MB.** see *Megabyte*.

**megabyte.** A unit of measure for storage capacity. For main storage, 1 megabyte equals 1 048 576 bytes (1024 x 1024); for auxiliary storage (disk, diskette, and tape), 1 megabyte equals 1 000 000 bytes (1000 x 1000).

**megahertz (MHz).** A unit of measure of frequency. One megahertz equals 1 000 000 hertz.

**MES.** See *miscellaneous equipment specification*.

**MHz.** See *megahertz*.

**MIB.** See *management information base*.

**mirroring cluster.** See *geographic cluster*.

**miscellaneous equipment specification (MES).** Any equipment that is added after the time of the initial order.

**modulation.** (1) The process by which a characteristic of a carrier is varied in accordance with a characteristic of an information-bearing signal (T). (2) The process by which a message signal is impressed upon a carrier signal so that the carrier is altered to represent the message signal.

**multicast address.** A type of IP address, which identifies a group of interfaces and permits all of the systems that are in that group to receive the same packet of information.

**multimode optical fiber.** (1) A graded-index or step-index optical fiber that allows more than one bound mode to propagate (E). Contrast with *single-mode optical fiber*. (2) In FDDI, an optical-fiber waveguide usually characterized by a core diameter of 50 - 100 microns that will allow a large number of modes to propagate.

**multiplexing.** In data transmission, a function that permits two or more data sources to share a common transmission medium so that each data source has its own channel (A) (I).

## N

**N.** See *newton*.

**NAS.** See *network-attached storage*.

**NetBIOS.** A standard interface to networks, IBM personal computers (PCs), and other compatible PCs. It is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS need not manage the details of LAN data-link-control protocols.

**network-attached storage (NAS).** A task-optimized storage device directly attached to a network that operates independently of the general-purpose file servers.

**Network File System (NFS).** A protocol, developed by Sun Microsystems, Incorporated, that allows any host in a network to mount another host's file directories. After a file directory is mounted, it appears to reside on the local host.

**network information services (NIS).** A set of UNIX network services (for example, a distributed service for retrieving information about the users, groups, network addresses, and gateways in a network) that resolve naming and addressing differences among computers in a network.



**newton (N).** The unit of force required to impart an acceleration of one meter per second per second to a mass of one kilogram (1 m/s<sup>2</sup>).

**NFS.** See *Network File System*.

**NIS.** See *network information services*.

**node.** A server participating in the cluster.

## O

**optical cable.** A fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications (E).

## P

**parity check.** (1) A redundancy check by which a recalculated parity bit is compared to the pre-given parity bit (T). (2) A check that tests whether the number of ones (or zeros) in an array of binary digits is odd or even (A).

**patch cable.** A length of cable with data connectors at both ends; it is normally used to interconnect two sections of building cable at a distribution panel or to connect a product to the building cable.

**path.** In a network, a route between two nodes.

**path group.** A collection of equivalent paths. Storage devices may have one - *n* path groups.

**PCI.** See *Peripheral Component Interconnect*.

**peer node.** When clustering, the second node at the site; not used for configuration.

**Peripheral Component Interconnect (PCI).** A local bus for PCs from Intel that provides a high-speed data path between the CPU and up to 10 peripherals (video, disk, network, and so on). The PCI bus coexists in the PC with the industry standard architecture (ISA) or extended industry standard architecture (EISA) bus. ISA and EISA boards plug into an ISA or EISA slot, while high-speed PCI controllers plug into a PCI slot.

**port.** See *socket*.

**port number.** (1) In Internet communications, the identification of an application entity to the transport service. (2) In the Internet suite of protocols, the identifier for a logical connector between an application entity and the transport service.

**primary node.** The node used to configure the remaining nodes in a cluster. There is a local primary node and a remote primary node.

**protocol.** The meaning of, and the sequencing rules for, requests and responses used for managing a network, transferring data, and synchronizing the states of network components.

**PSM.** See *Persistent Storage Manager*.

## R

**RAID.** See *redundant array of independent disks*.

**RAM.** See *random access memory*.

**random access memory (RAM).** A temporary storage location in which the central processing unit (CPU) stores and executes its processes. Contrast with *direct access storage device (DASD)*.

**Redundant Array of Independent Disks (RAID).** A method of protecting data loss due to disk failure based on the Redundant Array of Independent Disks specification published by the University of California in 1987. See also *device parity protection*.

**resource.** Cluster entity, such as a disk, file system, or network adapter, that is made highly available in the cluster.

**resource group.** A set of resources handled as one unit.

**router.** An attaching device that connects two LAN segments at the reference-model network layer. The LAN segments may use similar or different architectures.

## S

**SAN.** See *storage area network*.

**SCSI.** See *small computer system interface*.

**SDLC.** See *synchronous data link control*.

**server.** (1) In a network, a node that provides facilities to other stations; for example, a file server, a printer server, a mail server.

**service adapter or IP address.** The adapter and IP address used for client access; a “virtual” IP that will failover to another adapter or node.

**shielded twisted pair (STP).** A cable medium consisting of a telephone wire wrapped in a metal sheath to eliminate external interference.

**Simple Network Management Protocol (SNMP).** In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application-layer protocol. Information on devices managed is defined and stored in the application’s Management Information Base (MIB).

**single-mode optical fiber.** An optical fiber in which only the lowest-order bound mode (which can consist of a pair of orthogonally polarized fields) can propagate at the wavelength of interest. Contrast with *multimode optical fiber*.

**small computer system interface (SCSI).** A standard hardware interface that enables a variety of peripheral devices to communicate with one another.

**SNMP.** See *Simple Network Management Protocol*.

**storage area network (SAN).** A dedicated storage network tailored to a specific environment, combining servers, storage products, networking products, software, and services.

**socket.** In TCP/IP, the Internet address of the host computer on which the application runs, and the port number it uses. A TCP/IP application is identified by its socket.

**storage client network.** A classic, interconnected, fibre channel fabric with a single, fibre channel-fabric name.

**storage controller.** A device (such as a RAID controller) that creates and manages other storage devices. The circular arrangement between storage controllers and storage devices is due to the in-band management techniques used by the storage controllers.

**storage device.** A logical unit number (LUN) that terminates a collection of ports on the storage network.

**storage network.** An arrangement that provides shared access to a set of logical unit numbers (LUNs) across one - *n* storage client networks.

**storage port.** An engine’s connection point to a storage client network. A storage port is a member of a single fabric. See also *engine*.

**storage unit.** Hardware that contains one or more drive bays, power supplies, and a network interface. Some storage units contain RAID controllers; their storage unit is accessed by the NAS Gateway 500.

**STP.** See *shielded twisted pair*.

**synchronize.** Command that propagates the local node’s definition of the cluster to all other nodes of the cluster.

**synchronous data link control (SDLC).** A discipline for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

**synchronous data transfer.** A physical transfer of data to or from a device that has a predictable time relationship with the execution of an I/O request.

## T

**tape device.** A collection of tape units that share a model type and serial number (such as all the logical unit numbers (LUNs) of a tape library). See also *tape unit*.

**tape unit.** A tape device or a robotics controller that is visible over a storage network. A tape unit is a member of a single storage network (of 1 - *n* fabrics), but can have 1 - *n* equivalent paths.

**target.** A collection of logical units that are directly addressable on the network. The target corresponds to the server in a client-server model.

**TB.** see *Terabyte*.

**TCP.** See *Transmission Control Protocol*.

**TCP/IP.** See *Transmission Control Protocol/Internet Protocol*.

**teaming.** The grouping of two to four ports or adapters to increase transmission and reception throughput. Teaming creates a single, high-speed, fault-tolerant link that provides load balancing for both outbound and inbound traffic.

**Telnet.** In the Internet suite of protocols, a protocol that provides remote-terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

**terabyte.** For processor storage, real and virtual storage, and channel volume, 2 to the power of 40 or 1 099 511 627 776 bytes.

**thread.** A stream of computer instructions that is in control of a process. A multithread process begins with one stream of instructions (one thread) and may later create other instruction streams to perform tasks.

**timeout.** A time interval that is allotted for certain operations to occur, such as a response to polling or addressing before system operation is interrupted and must be restarted.

**Tivoli Storage Manager (TSM).** A client/server product that provides storage management and data access services in a heterogeneous environment.

**Transmission Control Protocol (TCP).** In TCP/IP, a host-to-host protocol that provides transmission in an Internet environment. TCP assumes Internet Protocol (IP) is the underlying protocol.

**Transmission Control Protocol/Internet Protocol (TCP/IP).** The Transmission Control Protocol and the Internet Protocol, which together provide reliable end-to-end connections between applications over interconnected networks of different types.

**TSM.** See *Tivoli Storage Manager*.

## U

**UPS.** see *uninterruptible power source*.

**uninterruptible power source.** A commercially available power source (usually a battery system) that provides temporary power to sustain the electrical operation of a device during a power failure until the normal power source can be restored.

**universal serial bus (USB).** A serial-interface standard for telephony and multimedia connections to personal computers.

**unshielded twisted pair (UTP).** A cable medium with one or more pairs of twisted insulated copper conductors bound in a single plastic sheath.

**USB.** See *universal serial bus*.

## V

**virtual local area network (VLAN).** A logical association of switch ports based upon a set of rules or criteria such as MAC addresses, protocols, network address, or multicast address. This concept permits resegmentation of the LAN without requiring physical rearrangement.

**virtual logical unit number (VLUN).** A subset of a logical drive.

**VLAN.** See *virtual local area network*.

**VLUN.** See *virtual logical unit number*.

**volume.** (1) A unit of storage on disk, tape, or other data-recording media. (2) A logical disk visible to the NAS Gateway 500 over a storage network. A volume is a member of a single storage network of 1 -  $n$  fabrics. It can have 1 -  $n$  path groups of 1 -  $n$  equivalent paths.

## W

**Windows Internet Naming Service (WINS).** A Microsoft program that provides a distributed database for registering and querying dynamic NetBIOS names to IP address mapping in a routed network environment.

**WINS.** See *Windows Internet Naming Service*.

**Windows networking.** A networking file-system protocol for the Windows operating system.

## X

**Xmodem.** A public-domain asynchronous data link control (DLC) protocol that provides packet numbering and checksum error control for the transfer of binary files.

---

# Index

## Numerics

- 7852–400 modem, configuring 256
- 7857–017 modem, configuring 256
- 7858–336 modem, configuring 256

## A

- about this manual xvii
- accessibility xxii
- accessing
  - basic configuration interface 215
- adapters and interfaces, networking 149
- add
  - machine 222
- adding
  - administrator 91
  - cluster 244
  - fibre channel HBA 243
  - network adapter 243
  - new hardware 243
  - or changing user's key 154
  - Remote Mirroring 244
  - volume to export list 132
- adding a NetBIOS name
  - NetBIOS 147
- administration tasks 251
- administrator
  - managing 91
  - NAS 6
- advanced ASCII user interfaces, basic 201
- alert
  - E-mail template 236
- analyzing INSTALLP faults 206
- applications, managing
  - backup 94
  - configuring the TSM client 93
  - configuring Tivoli SAN Manager 96
  - configuring TSM storage agent 95
  - configuring TSRM agent 98
  - dumping SNMP information 100
  - getting SNMP information 99
  - managing using TSM 93
  - restore 94
  - setting SNMP information 100
  - setting the password for Tivoli SAN Manager agent 97
  - showing or changing boot state of Tivoli SAN Manager agent 97
  - showing or changing the boot state of TSM storage agent 96
  - showing or changing the state of the TSRM agent 99
  - starting and stopping the TSM storage agent 95
  - starting and stopping Tivoli SAN Manager agent 97
  - starting and stopping TSRM agent 98
  - starting SNMP 100
  - stopping SNMP 100

- applications, managing (*continued*)
  - using SNMP 99
  - using TSANM 96
  - using TSRM 98
- ASCII user interfaces, basic and advanced 201
- authentication
  - CIFS server 141
- authentication, CIFS 138

## B

- backing up a NetBIOS Name table
  - NetBIOS 148
- backing up configuration files 157
- backup 94
- backup and recovery 157
- backup and recovery procedures
  - recovery back to manufacturing state 193
- basic
  - and advanced ASCII user interfaces 201
  - configuration 216
  - configuration interface 215
  - Electronic Service Agent configuration 212
- basic setup
  - CIFS 140
- boot and shutdown 157

## C

- call controller property 231
- call home 195
- CD-ROMs, System Software Recovery and Supplementary 187
- central database 199
- change or show attributes 134
- changing
  - administrator's password 91
  - and showing date and time 159
  - attributes of CIFS shares 144
  - CIFS user 146
  - dump options 161
  - encryption key 155
  - reboot options 158
  - time zone 159
  - to SNMP V3 251
  - user's key 154
  - volumes 167
  - volumes command 167
- Changing the NIS domain name
  - NIS host 106
- characteristics of an administrator 92
- CIFS
  - authentication 138, 141
  - basic setup 140
  - changing attributes of shares 144
  - changing password 146
  - changing user 146

- CIFS *(continued)*
  - concepts 138
  - creating a user 145
  - creating shares 143
  - fileserver characteristics 142
  - listing shares 143
  - listing users 144
  - mapping file access users 145
  - network file serving 4
  - removing CIFS shares 144
  - removing user 146
  - resource limits 142
  - server statistics 139
  - server status 139
  - starting server 139
  - stopping server 139
  - user mapping 138
  - wizard 53
- CLI commands
  - change volume using chvol 167
  - copy volume using cpvol 170
  - create volume using mkvol 166
  - defragment volume 168
  - delete volume using rmvol 168
  - displaying HTTP server configuration information 129
  - displaying HTTP server logs 130, 131
  - displaying remotely mounted filesystems 136
  - export volume using expvol 168
  - extend volume 169
  - import volume 169
  - list volume using lsvol 172
  - mirror volume using mirvol 171
  - mount volume using mountvol 170
  - replace volume using replacevol 170
  - starting HTTP administration server daemon 129
  - starting HTTP server daemon 129
  - starting PC NFS 136
  - stopping PC NFS 137
  - synchronize volume using syncvol 171
  - unmirror volume using mirvol -u 171
  - unmount volume using unmountvol 171
  - viewing volume statistics using volstat 172
- client access, managing 101
- client code, manually installing the Electronic Service Agent 208
- cluster
  - adding 244
  - deleting 111
  - disabling 110, 112
  - disabling a volume 114
  - enabling 110
  - enabling a volume 114
  - enabling on single node 112
  - log viewing 115
  - managing 109
  - modifying 116
  - moving service to another adapter 113
  - optional feature 4
  - relocating volumes 113
  - showing node state 111
- cluster *(continued)*
  - showing volumes served 113
  - synchronizing 111
  - tasks 109
  - verifying 110
  - wizard 43
- command line installation 206
- command shortcuts 259
- commands
  - CLI
    - copy volume 170
    - create volume using mkvol 166
    - defragmenting 168
    - deleting volume 168
    - displaying remotely mounted filesystems 136
    - export volume 168
    - extend volume using extendvol 169
    - import volume using impvol 169
    - listing 172
    - mirror volume 171
    - mount volume 170
    - replacevol 170
    - starting PC NFS 136
    - stopping PC NFS 137
    - synchronize 172
    - synchronize volume 171
    - unmirroring volume 171
    - unmount volume 171
    - viewing volume statistics 172
    - volume, changing 167
  - listing 172
  - mirroring 171
- SMIT fastpath
  - changing 167
  - changing NFS characteristics 132
  - copying 170
  - defragmenting 168
  - deleting 168
  - displaying HTTP server configuration information 129
  - displaying HTTP server logs 130
  - displaying remotely mounted filesystems 136
  - exporting 168
  - extending 169
  - importing 169
  - mounting 170
  - replacing 170
  - start HTTP administration server daemon 129
  - start HTTP server daemon 129
  - starting PC NF 137
  - starting PC NFS 137
  - volume create 167
- unmirroring 171
- unmounting 171
- viewing statistics 173
- volumes
  - listing 172
  - mirroring 171
  - synchronizing 171
  - unmirroring 171
  - unmounting 170

- commands *(continued)*
  - volumes *(continued)*
    - viewing statistics 172
- WebSM
  - adding a new administrator 91
  - changing 167
  - changing an administrator's password 92
  - copying 170
  - creating volumes 167
  - defragmenting 168
  - deleting 168
  - exporting 168
  - extending 169
  - importing 169
  - listing 172
  - listing administrators 92
  - mirroring 171
  - mounting 170
  - replacing 170
  - synchronize 172
  - unmirroring 171
  - unmounting 171
  - viewing statistics 173
- common tasks
  - creating NAS volumes 89
  - creating users 89
  - protecting you system data 90
- concepts, CIFS 138
- configuration
  - basic Electronic Service Agent 212
  - property parameter details 227
- configuring
  - 7857-017 modem 256
  - 7858-336 modem 256
  - devices 119
  - HTTP server 126
  - LDAP client 107
  - NAS volumes 166
  - network adapters, using TCP/IP 150
  - NIS client 105
  - NIS+ client 106
  - physical volumes 166
  - snapshot schedule 181
  - Tivoli SAN Manager agent 96
  - TSM client 93
  - TSM storage agent 95
  - TSRM agent 98
- configuring the 7852-400 modem 256
- connection manger property 232
- copying volumes 169
- creating
  - CIFS shares 143
  - CIFS users 145
  - HTTP file shares 128
  - NAS volumes 89
  - snapshot 178
  - users 89
  - volumes 166

## D

- database, central 199
- decrypting and storing key 154
- definitions, user 5
- defragmenting volumes 168
- deleting
  - cluster 111
  - snapshot 179
  - stored key 154
  - volumes 167
- deleting a NetBIOS name
  - NetBIOS 147
- deleting a NetBIOS name and IP address
  - NetBIOS 147
- devices
  - changing EtherChannel/IEEE 802.2ad link aggregation 124
  - configuring 119
  - creating link aggregation device 123
  - displaying disk size 121
  - displaying disks and attributes 120
  - displaying installed and attributes 121
  - displaying size of remote disk 122
  - displaying specific information 121
  - listing link aggregation 123
  - managing 119
  - removing EtherChannel/IEEE 802.2ad link aggregation 124
  - removing volume information 122, 123
  - task to manage storage 119
  - unconfiguring 120
- dialer property 233
- directory services 104
- disabling
  - cluster 112
  - volumes 114
- disabling a cluster 110
- displaying
  - configured disks and attributes 120
  - device specific information 121
  - disk size 121
  - exported volumes 132
- dump options, changing 161
- dumping SNMP information 100

## E

- E-mail alert template 236
- Electronic Server System process 200
- Electronic Service Agent
  - basic configuration 216
  - client code, installing manually 208
  - configuration, basic 212
  - installation command line 206
  - installation failure 206
  - installing 205
  - prerequisites 202
  - unsupported devices 198
- enabling a cluster 110
- enabling a volume 114

- enroll property 235
- export
  - all volumes 134
  - remove volumes 135
  - specific volume 134
- exporting and recovering snapshot data 133
- exporting volumes 168
- extending volumes 169

## F

- failure, Electronic Service Agent installation 206
- fastpath commands, SMIT 259
- fastpath, SMIT menu 80
- faults, analyzing INSTALLP 206
- feature selection wizard 25
- Fibre channel HBA, adding 243
- file access user
  - adding a group 103
  - adding local 101
  - changing local password 102
  - changing or showing characteristics of group 103
  - changing or showing local characteristics 102
  - listing all groups 104
  - listing local 103
  - removing a group 103
  - removing local 102
  - setting or changing a CIFS user's password 103
- file access users
  - CIFS access 6
  - FTP access 6
  - HTTP access 6
  - NFS access 6
- file serving, managing 125
- fileserver characteristics
  - CIFS server 142
- firmware 248
  - level 248
  - update 248
- firmware updates
  - system 248
- first time powering on 13
- FTP
  - create login 125
  - create users 125
  - enable login 125
  - manage users 125

## G

- general setup wizard 33
- getting SNMP information 99
- getting started 13

## H

- HTTP
  - configuring server 126
  - creating file shares 128
  - managing users 127

## I

- importing volumes 169
- initial configuration wizard 21
- installation and packaging updates 246
- installation failure 206
- installing
  - client code, manually 208
  - Electronic Service Agent 205
  - Electronic Service Agent from SMIT 205
  - Web-based System Manager Remote Client 15
- installing a system backup using a tape device 192
- INSTALLP faults, analyzing 206
- installp message flow 207
- interface
  - accessing the basic configuration 215
  - basic and advanced ASCII user 201
- inventory scout 239

## L

- LDAP client
  - configuring 107
  - removing configuration 108
- list administrators 92
- listing
  - CIFS shares 143
  - network adapters and interfaces 149
  - users 144
- listing command 172
- listing names in the NetBIOS Name Table
  - NetBIOS 147
- local
  - adding a file access user 101
  - adding a group 103
  - changing file access user password 102
  - changing or showing characteristics of group 103
  - characteristics, changing or showing file access user 102
  - file access user 101
  - listing all groups 104
  - listing file access user 103
  - removing a group 103
  - removing file access user 102
  - setting or changing a CIFS user's password 103

## M

- machine
  - add 222
  - remove 224
- managing
  - administrators 91
  - clusters 109
  - devices 119
  - file serving 125
  - HTTP users 127
  - NAS volumes 165
  - networking 149
  - security 153
  - snapshots 165, 178



- managing applications
  - backup 94
  - configuring the TSM client 93
  - configuring Tivoli SAN Manager agent 96
  - configuring TSM storage agent 95
  - configuring TSRM agent 98
  - dumping SNMP information 100
  - getting SNMP information 99
  - restore 94
  - setting SNMP information 100
  - setting the password for Tivoli SAN Manager agent 97
  - showing or changing boot state of Tivoli SAN Manager agent 97
  - showing or changing the boot state of TSM storage agent 96
  - showing or changing the state of the TSRM agent 99
  - starting and stopping the TSM storage agent 95
  - starting and stopping Tivoli SAN Manager agent 97
  - starting and stopping TSRM agent 98
  - starting SNMP 100
  - stopping SNMP 100
  - using SNMP 99
  - using TSANM 96
  - using TSM 93
  - using TSRM 98
- manual, about this xvii
- manual, who should read xvii
- mapping file access users 145
- message flow, installp 207
- modem
  - 7852–400, configuring 256
  - 7857-017 modem configuring 256
  - 7858–336, configuring 256
  - configurations 255
  - setup 255
- modifying cluster 116
- monitored network 199
- monitoring system 200
- mounting a NAS volume 170
- moving cluster service 113

## N

- NAS administrator common tasks 89
- NAS administrators 6
- NAS Gateway 500 library xviii
- NAS volume management 165
- NAS Volume Wizard 59
- NAS volumes
  - changing 167
  - configuring 166
  - configuring physical 166
  - copying 169
  - creating 166
  - defragmenting 168
  - deleting 167
  - exporting 168
  - extending 169
  - importing 169

- NAS volumes (*continued*)
  - listing 172
  - managing 165
  - mirroring 171
  - mounting 170
  - replacing 170
  - synchronizing 171
  - unmirroring 171
  - unmounting 170
  - viewing statistics 172
- NetBIOS
  - adding a NetBIOS name 147
  - backing up a NetBIOS Name table 148
  - deleting a NetBIOS name 147
  - deleting a NetBIOS name and IP address 147
  - listing names in the NetBIOS Name Table 147
  - restoring a NetBIOS Name table 148
- NetBIOS Name Server 147
- network
  - adapter, adding 243
  - configuration wizard 41
  - interface statistics 150
  - monitored 199
- network property 227
- networking
  - configuring adapters 150
  - listing adapters and interfaces 149
  - managing 149
  - managing tasks 149
- new hardware, adding 243
- NFS
  - adding volume to export list 132
  - change or show attribute 134
  - changing characteristics 131
  - displaying exported volumes 132
  - export all volumes 134
  - export specific volume 134
  - exporting and recovering snapshot data 133
  - starting 131
  - stopping 131
  - unexport a specific volume 135
  - unexport all volumes 135
  - unexport or remove volumes 135
- NFS and NIS security tasks 153
- NIS client configuration, removing 106
- NIS client, changing or showing characteristics 105
- NIS client, configuring 105
- NIS host, changing the NIS domain name 106
- NIS+
  - credential administration 107
  - initializing for a NIS+ client 106
- NIS+ client configuration, removing 107
- NIS+ client, configuring 106
- ntpdate command 160
- ntpq command 160

## O

- On Demand Server process 200
- optional features
  - CIFS network file serving 4

optional features (*continued*)  
cluster 4

## P

panel  
add or delete NAS administrators 35  
CIFS server identification 53  
CIFS user authentication 55  
features selection 25  
file access user 38  
List of Directory Services 36  
network configuration 41  
NIS client configuration 37  
set date and time 33  
set root password 34  
static or dynamic IP address selection 42  
volume selection 60  
Web-based System Manager Remote Client Install  
Image Download 16  
WebSM navigation and contents panel 84  
WebSM Welcome 43  
Windows Internet name service 54  
parameter details, configuration property 227  
password  
changing CIFS user 146  
changing file access user 102  
performing basic configuration 216  
physical volumes, configuring 166  
power supply  
configuring uninterruptible 241  
uninterruptible 241  
powering on, first time 13  
prerequisites for Electronic Service Agent 202  
problem determination 160  
process  
Electronic Server System 200  
On Demand Server 200  
property  
call controller 231  
connection manger 232  
dialer 233  
enroll 235  
network 227  
parameter details, configuration 227  
protecting your system data 90  
publications  
hardcopy publications xix  
softcopy publications xix  
translated publications xx

## Q

quick start for setting up, configuring, administering the  
NAS Gateway 500 13

## R

Recovery and Supplementary CD-ROMs, using 187  
recovery back to manufacturing state 193  
relocating volumes 113

Remote Client, starting WebSM  
Linux 19  
Windows 19  
Remote Mirroring  
adding 244  
remove  
machine 224  
removing  
CIFS shares 144  
CIFS user 146  
LDAP client configuration 108  
NIS client configuration 106  
NIS+ client configuration 107  
volume information 122, 123  
renaming a snapshot 179  
replacing volumes 170  
resource limits  
CIFS server 142  
restore 94  
restore configuration files 157  
restoring up a NetBIOS Name table  
NetBIOS 148  
Reviewing the installp message flow 207  
roll back a snapshot 180  
root user 5, 6  
running wizards after initial configuration  
CIFS wizard 71  
cluster wizard 71  
feature selection wizard 71  
file access user wizard 71  
link aggregation wizard 71  
NAS administrator wizard 71  
remote mirror wizard 71  
volume wizard 71

## S

security  
adding or changing user's key 154  
changing encryption key 155  
decrypting and storing key 154  
deleting stored key 154  
managing 153  
NFS and NIS tasks 153  
starting keysevd daemon 153  
stopping keysevd daemon 154  
send  
Vital Product Data (VPD) 225  
server statistics  
CIFS server 139  
server status  
CIFS server 139  
services directory 104  
set date and time 158  
setting SNMP information 100  
setting the password for Tivoli SAN Manager agent 97  
setting up, configuring, administering the NAS Gateway  
500, quick start 13  
setup modem 255  
showing  
cluster node state 111

- showing *(continued)*
    - or changing boot state of Tivoli SAN Manager agent 97
    - or changing the boot state of TSM storage agent 96
    - or changing the boot state of TSRM agent 99
    - snapshot schedule 182
    - volumes served 113
  - showing configuration
    - NIS client 105
  - shutdown system 158
  - single node, enabling clustering 112
  - skills needed to install, configure, and administer this product xvii
  - SMIT
    - installing Electronic Service Agent 205
    - menu fastpaths 80
    - using 79
  - SMIT fastpath
    - changing, 167
    - copying command 170
    - defragmenting command 168
    - deleting command 168
    - displaying remotely mounted filesystems 136
    - exporting command 168
    - extending command 169
    - importing command 169
    - listing command 172
    - mirroring 171
    - mounting command 170
    - replacing command 170
    - starting PC NF 137
    - starting PC NFS 137
    - synchronize command 172
    - unmirroring command 171
    - unmounting 171
    - viewing statistics command 173
    - volume create command 167
  - SMIT fastpath commands 259
  - snapshots
    - configuring schedule 181
    - creating 178
    - deleting 179
    - managing 165, 178
    - managing schedule 182
    - renaming 179
    - roll back 180
    - showing schedule 182
  - SNMP
    - getting information 99
    - information dumping 100
    - setting information 100
    - starting 100
    - stopping 100
    - using 99
  - SNMP V3
    - changing to 251
    - dual node 251
    - single node 251
  - software system upgrades 246
  - software update practices 247
  - starting
    - CIFS server 139
    - keyserv daemon 153
    - NFS 131
    - SNMP 100
    - Tivoli SAN Manager agent 97
    - TSM storage agent 95
    - TSRM agent 98
    - WebSM Remote Client
      - Linux 19
      - Windows 19
  - stopping
    - CIFS server 139
    - keyserv daemon 154
    - NFS 131
    - SNMP 100
    - Tivoli SAN Manager agent 97
    - TSM storage agent 95
    - TSRM agent 98
  - synchronize command 172
  - synchronizing the cluster 111
  - system
    - backing up configuration files 157
    - backup and recovery 157
    - boot and shutdown 157
    - changing and showing date and time 159
    - changing reboot options 158
    - changing time zone 159
    - managing the 157
    - monitoring 200
    - problem determination 160
    - restore configuration files 157
    - set date and time 158
    - shutdown 158
    - using ntpdate command 160
    - using ntpq command 160
  - system firmware updates 248
  - system upgrades and configuration changes 243
- ## T
- tasks to manage storage devices 119
  - tasks used to manage administrators 91
    - adding a new administrator 91
    - changing an administrator's password 91
    - list administrators 92
    - showing the characteristics of an administrator 92
  - tasks, administration 251
  - TCP/IP, configuring network adapters using 150
  - template
    - E-mail 236
  - testing uninterruptible power supply 241
  - Tivoli SAN Manager
    - showing or changing boot state 97
  - Tivoli SAN Manager agent
    - configuring 96
    - setting the password 97
    - starting and stopping 97
  - trademarks 314
  - TSANM, using 96
  - TSM client, configuring 93

- TSM storage agent
  - configuring 95
  - showing or changing the boot state 96
  - starting and stopping 95
- TSRM agent
  - configuring 98
  - showing or changing the boot state 99
  - starting and stopping, 98
- TSRM, using 98
- types of update packages 247

## U

- unconfiguring devices 120
- unexport a specific volume 135
- unexport all volumes 135
- uninterruptible power supply 241
  - configuring 241
  - testing 241
- unmirroring command 171
- unsupported devices, Electronic Service agent 198
- update packages 247
- updates, installation and packaging 246
- upgrading your NAS Gateway 500 system
  - software 246
- user
  - definitions 5
  - file access 6
  - interfaces, basic and advanced ASCII 201
  - mapping, CIFS 138
  - NAS administrator 6
  - root 5
- users of this manual xvii
- using the System Software Recovery CD-ROM 193

## V

- VDP 225
- verifying clusters 110
- viewing cluster log 115
- viewing statistics command 173
- Vital Product Data (VPD), send 225
- volumes
  - changing 167
  - copying 169
  - creating 166
  - defragmenting 168
  - deleting 167
  - exporting 168
  - extending 169
  - importing 169
  - listing 172
  - management 165
  - mirroring 171
  - mounting NAS 170
  - relocating 113
  - replacing 170
  - synchronizing 171
  - unmounting command 170
  - viewing statistics 172

## W

- Web sites xxii
  - firmware updates 248
  - microcode updates 248
- Web-based System Manager Remote Client
  - installing 15
    - Linux 15
    - requirements 15
    - Windows 15
- Web-based System Manger Remote Client
  - starting
    - Linux 19
    - Windows 19
- WebSM 171, 172, 173
  - adding a new administrator 91
  - changing an administrator's password 92
  - changing command 167
  - copying command 170
  - creating volumes 167
  - defragmenting command 168
  - deleting command 168
  - exporting command 168
  - extending command 169
  - importing command 169
  - listing administrators 92
  - mirroring command 171
  - mounting command 170
  - replacing command 170
  - unmounting command 171
  - using after initial configuration 83
- WebSM commands 259
- who should read this manual xvii
- wizard
  - CIFS 21, 53
  - cluster 21, 43
  - Feature 21
  - General system 21
  - initial configuration 21
  - Network configuration 21
  - volumes 21





Part Number: 24R1380

Printed in USA

SC30-4072-01



(1P) P/N: 24R1380

